



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**ESTABLISHING VIABLE AND EFFECTIVE  
INFORMATION-WARFARE CAPABILITY IN DEVELOPING  
NATIONS BASED ON THE U.S. MODEL**

by

Ashar Ahmed Khan Niazi

December, 2012

Thesis Advisor:

Co-Advisor:

Steve Iatrou

Edward L. Fisher

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2012	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE ESTABLISHING VIABLE AND EFFECTIVE INFORMATION-WARFARE CAPABILITY IN DEVELOPING NATIONS BASED ON THE U.S. MODEL			5. FUNDING NUMBERS	
6. AUTHOR(S) Ashar Ahmed Khan Niazi				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____ N/A ____.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words)  Information Warfare (IW) is a reality of the 21st century. With the advancements in computer technology and innovations in information systems and networks, information has become a forceful weapon and an element of national power. Consequently, the conduct of war in this age has been greatly affected by the manner in which the information is treated by the opposing forces. The United States Department of Defense (DoD) has been aggressively formulating doctrine and policy on the subject since the early 1990s. The study of this evolution offers guidelines to other coalition partners who may wish to make their own organizations effective and viable by incorporating changes to suit their scale and scope of operations.  IW, now called information operations in the U.S. DoD, is the amalgamation of multiple independent and diverse capabilities. It will be explored that some of the latest IW capabilities may make less of a contribution in developing countries where organizations are less dependent on advanced information systems and communication networks in the cyber domain. This thesis will describe U.S. IO implementation methodology and in the end identify feasible IW capabilities in the backdrop of developing countries. A simplistic IW operational model will also be presented for consideration in counterinsurgency and counterterrorism campaigns.				
14. SUBJECT TERMS Information Warfare, Information Operations, IO capabilities, Core capabilities, Supporting capabilities, Related capabilities, IO implementation in U.S. armed services, IO organization, IW in smaller militaries, Feasible IW adaptation, IW operational model.			15. NUMBER OF PAGES 131	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**ESTABLISHING VIABLE AND EFFECTIVE INFORMATION WARFARE  
CAPABILITY IN DEVELOPING NATIONS BASED ON THE U.S. MODEL**

Ashar Ahmed Khan Niazi  
Commander, Pakistani Navy  
BSc (Honours) Naval Sciences, Karachi University, 1999  
MSc War Studies (Maritime), National Defense University, Islamabad, 2010

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN  
INFORMATION WARFARE SYSTEMS ENGINEERING**

from the

**NAVAL POSTGRADUATE SCHOOL  
December 2012**

Author: Ashar Ahmed Khan Niazi

Approved by: Steven Iatrou  
Thesis Advisor

Edward L. Fisher  
Thesis Co-Advisor

Dan Boger  
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Information Warfare (IW) is a reality of the 21st century. With the advancements in computer technology and innovations in information systems and networks, information has become a forceful weapon and an element of national power. Consequently, the conduct of war in this age has been greatly affected by the manner in which the information is treated by the opposing forces. The United States Department of Defense (DoD) has been aggressively formulating doctrine and policy on the subject since the early 1990s. The study of this evolution offers guidelines to other coalition partners who may wish to make their own organizations effective and viable by incorporating changes to suit their scale and scope of operations.

IW, now called information operations in the U.S. DoD, is the amalgamation of multiple independent and diverse capabilities. It will be explored that some of the latest IW capabilities may make less of a contribution in developing countries where organizations are less dependent on advanced information systems and communication networks in the cyber domain. This thesis will describe U.S. IO implementation methodology and in the end identify feasible IW capabilities in the backdrop of developing countries. A simplistic IW operational model will also be presented for consideration in counterinsurgency and counterterrorism campaigns.

THIS PAGE INTENTIONALLY LEFT BLANK



# TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	FOREWORD .....	1
B.	PURPOSE.....	2
C.	THE NATURE OF INFORMATION WARFARE .....	3
D.	THESIS OVERVIEW .....	4
	1. Scope of the Study .....	4
	2. Thesis Organization .....	4
II.	CONCEPTUAL UNDERSTANDING OF THE TERM “IW” .....	7
A.	SCOPE/DIMENSIONS OF IW .....	7
B.	NON-MILITARY/CIVIL PERSPECTIVE OF IW .....	9
	1. Personal Information Warfare.....	10
	2. Commercial Information Warfare: .....	10
	3. Global Information Warfare.....	10
C.	THE MILITARY PERSPECTIVE OF IW .....	10
	1. Distinguishing IW from IO.....	10
	2. The Targets of Information Warfare .....	14
D.	INFORMATION CAMPAIGN IN INFORMATION OPERATIONS VIS-A-VIS PERCEPTION MANAGEMENT.....	15
III.	U.S. JOINT AND SERVICES LEVEL INTERPRETATION OF INFORMATION OPERATIONS .....	19
A.	INTRODUCTION .....	19
B.	JOINT FORCES COMMAND PERSPECTIVE ON IO.....	19
	1. Important Terminology Used in IO Literature.....	19
	2. Defining IO.....	21
C.	CAPABILITIES INVOLVED IN IO .....	22
	1. Core Capabilities .....	23
	2. Supporting Capabilities.....	24
	3. Related Capabilities.....	24
	4. Core Capabilities in IO .....	25
	a. <i>Military Information Support Operations (MISO)</i> .....	25
	b. <i>Military Deception (MILDEC)</i> .....	25
	c. <i>Operations Security</i> .....	26
	d. <i>Electronic Warfare</i> .....	26
	e. <i>Computer Network Operations</i> .....	27
D.	INFORMATION OPERATIONS SUPPORTING CAPABILITIES .....	28
	1. Information Assurance.....	28
	2. Physical Security .....	28
	3. Physical Attack .....	29
	4. Counterintelligence .....	29
	5. Human Intelligence.....	29
	6. Combat Camera .....	30

E.	INFORMATION-OPERATIONS-RELATED CAPABILITIES .....	30
1.	Public Affairs.....	30
2.	Civil–Military Operations.....	31
3.	Defense Support to Public Diplomacy.....	31
F.	COMPARATIVE CHARACTERISTICS OF IO TERMS IN U.S. DOCTRINE: USAF FOCUS ON INFLUENCE OPS AND TECHNICAL CAPABILITIES.....	32
G.	THE U.S. NAVY’S MOVE TOWARD INFORMATION DOMINANCE .....	34
H.	ESTABLISHMENT OF THE NAVY’S INFORMATION-DOMINANCE CORPS.....	35
I.	THE U.S. ARMY’S MOVES TOWARD INFORM-AND-INFLUENCE ACTIVITIES.....	38
J.	THE U.S. MARINE CORPS (USMC’S) APPROACH TO IO .....	42
K.	SUMMARY .....	43
IV.	U.S. JOINT AND SERVICE LEVEL IMPLEMENTATION OF INFORMATION OPERATIONS .....	45
A.	INTRODUCTION.....	45
B.	IO ORGANIZATION AT THE U.S. JOINT-STAFF LEVEL .....	46
1.	General .....	46
2.	Organization.....	47
a.	<i>Computer Network Operations Division (CNOD) .....</i>	47
b.	<i>Information Operations Division (IOD).....</i>	48
c.	<i>Military Information Support Division (MISD).....</i>	48
d.	<i>Special Actions Division (SAD) .....</i>	48
e.	<i>Joint Information Operations Warfare Center (JIOWC).....</i>	48
C.	REORGANIZATION OF IO IN THE U.S. DOD .....	49
D.	U.S. STRATEGIC COMMAND (USSTRATCOM) .....	50
1.	Mission .....	50
2.	History .....	51
3.	Command Subcomponents. ....	52
E.	U.S. SPECIAL OPERATIONS COMMAND (USSOCOM) .....	53
1.	Mission .....	53
2.	History .....	53
3.	IO Core and Related Capabilities within USSOCOM Purview.....	54
a.	<i>Military Information Support Operations (MISO).....</i>	54
b.	<i>Civil Affairs (CA) .....</i>	54
c.	<i>Components .....</i>	55
F.	IO ORGANIZATION IN THE U.S. ARMED SERVICES .....	55
1.	The U.S. Army .....	55
2.	The U.S. Navy.....	56
3.	The U.S. Air Force.....	57
4.	The U.S. Marine Corps .....	58

G.	SUMMARY .....	59
V.	ESTABLISHING A VIABLE INFORMATION WARFARE CAPABILITY IN SMALLER MILITARIES.....	61
A.	INTRODUCTION .....	61
B.	INFORMATION WARFARE POLICY AND STRATEGY .....	61
1.	General .....	61
2.	Security Policy .....	64
3.	Security Strategy .....	66
C.	FEASIBLE IW ADAPTATION FOR SMALLER MILITARIES.....	68
1.	Insurgencies and Terrorist Activities in Developing Countries.....	69
2.	The IW Capabilities with the Greatest Benefit for Smaller Militaries .....	72
3.	Shaping Perceptions with the Help of IW .....	73
4.	A Simplistic Operational Model of Information Warfare.....	77
D.	SUMMARY .....	80
VI.	SUMMARY, RECOMMENDATIONS AND CONCLUSION.....	83
A.	SUMMARY .....	83
B.	RECOMMENDATIONS .....	84
1.	Policy Formulation by Government and Military leaders ...	85
2.	Making Comprehensive IW strategy .....	85
3.	Managing the Perceptual Level through IW .....	85
4.	Systematic Development of IW Capabilities.....	86
5.	Organizing CMO, PSYOP and PA .....	86
6.	Cooperation and Coordination .....	86
C.	CONCLUSION .....	87
APPENDIX A.	U.S. UNIFIED COMMAND PLAN (UCP) AND COMBATANT COMMANDS (COCOMS) .....	89
A.	COMBATANT COMMAND (COCOM) .....	89
1.	Functional Combatant Commands .....	90
2.	Geographic Combatant Commands.....	91
3.	Command Authority .....	92
4.	Organizational Principles.....	94
APPENDIX B.	U.S. STRATEGIC COMMAND'S SUBCOMPONENTS .....	97
A.	FUNCTIONAL COMPONENTS .....	97
1.	U.S. Cyber Command (USCYBERCOM).....	97
2.	Joint Functional Component Command—Global Strike (JFCC-GS).....	97
3.	Joint Functional Component Command—Space (JFCC- Space).....	97
4.	Joint Functional Component Command—Integrated Missile Defense (JFCC-IMD) .....	98
5.	Joint Functional Component Command—Intelligence, Surveillance and Reconnaissance (JFCC-ISR) .....	98

6.	USSTRATCOM Center for Combating Weapons of Mass Destruction (SCC–WMD).....	98
7.	Joint Warfare Analysis Center (JWAC).....	98
B.	SERVICE COMPONENTS .....	98
1.	Air Force Global Strike Command (AFGSC).....	98
2.	U.S. Army Forces Strategic Command (ARSTRAT).....	99
3.	Fleet Forces Command .....	99
4.	Marine Corps Forces U.S. Strategic Command (MARFORSTRAT).....	99
5.	Air Force Space Command (AFSPC) .....	99
APPENDIX C.	U.S. SPECIAL OPERATIONS COMMAND'S SUBCOMPONENTS.....	101
1.	U.S. Army Special Operations Command (USASOC) .....	101
2.	Naval Special Warfare Command (NSWC).....	101
3.	Air Force Special Operations Command (AFSOC) .....	102
4.	Marine Special Operations Command (MARSOC) .....	102
5.	Joint Special Operations Command (JSOC) .....	102
	LIST OF REFERENCES.....	103
A.	LITERATURE.....	103
B.	MILITARY PUBLICATIONS.....	103
C.	INTERNET SOURCES.....	105
	INITIAL DISTRIBUTION LIST .....	107

## LIST OF FIGURES

Figure 1.	National Elements of Power .....	8
Figure 2.	Differences in scope between IW and IO .....	12
Figure 3.	Perception management .....	16
Figure 4.	Components of an information campaign .....	17
Figure 5.	Capabilities involved in IO .....	23
Figure 6.	Communities merged to form the Information Dominance Corps (IDC) .....	37
Figure 7.	Army Inform-and-Influence Activities .....	39
Figure 8.	Integration of Information-Related Capabilities to affect the Information Environment .....	40
Figure 9.	Army Cyber/Electromagnetic Activities .....	41
Figure 10.	Military Organization of U.S. DoD .....	46
Figure 11.	Fundamental hierarchy and components of a national information-security strategy .....	65
Figure 12.	The strategic process includes strategy development and assessment elements .....	67
Figure 13.	Temporal trends in terrorism in the Global Terrorism Database (GTD). .....	71
Figure 14.	Capabilities Involved in Shaping Perception .....	74
Figure 15.	Functional Flow of a PSYOP Campaign .....	76
Figure 16.	A Simplistic Model for IO in Developing Countries .....	79
Figure 17.	U.S. COCOMS Area of Responsibility in 2011. ....	92
Figure 18.	U.S. COCOMS Chain of Command .....	94

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

Table 1.	The Range of Military Operations.....	13
Table 2.	Common Information-Operations Terms .....	34
Table 3.	General Hierarchy of Policy, Strategy, and Operations to Address IW's Military Perspective .....	63

THIS PAGE INTENTIONALLY LEFT BLANK



## LIST OF ACRONYMS AND ABBREVIATIONS

Note: All acronyms and abbreviations in the list are from U.S. Joint Publication 1–02 Department of Defense Dictionary of Military and Associated Terms 8 November 2010 (as amended through 15 July 2012) unless indicated otherwise.

ACC	Air Combat Command
AFGSC	Air Force Global Strike Command
AFSOC	Air Force Special Operations Command
AFSPC	Air Force Space Command
AFSPC	Air Force Space Command
ARSTRAT	United States Army Forces Strategic Command
BDA	battle damage assessment
C2W	command and control warfare
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
CA	civil affairs
CCA	chairman-controlled activity
CI	counter intelligence
CJCS	Chairman of the Joint Chiefs of Staff
CMC	Commandant of the Marine Corps
CMO	civil-military operations
CNA	computer-network attack
CND	computer-network defense
CNE	computer-network exploitation
CNO	Chief of Naval Operations; computer network operations

CNOD	Computer Network Operations Division
COCOM	combatant command (command authority)
COMCAM	combat camera
CSA	Chief of Staff, United States Army
CSAF	Chief of Staff, United States Air Force
DA	Department of the Army
DAF	Department of the Air Force
DCNO	Deputy Chief of Naval Operations
DDGO	Deputy Director for Global Operations (U.S. Army War College IO Primer)
DII	defense information infrastructure
DIME	diplomatic, informational, military, and economic power
DoD	Department of Defense
DODD	Department of Defense Directive
DON	Department of the Navy
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
DSPD	defense support to public diplomacy
EA	electronic attack
EM	electromagnetic
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
FCC	Fleet Cyber Command
FEA	front-end analysis

FM	field manual
FuOps	future operations—(U.S. Marine Corps Warfare Publication, MCWP 3–40.4, MAGTF Information Operations)
GII	global information infrastructure
GPS	Global Positioning System
HUMINT	human intelligence
IA	information assurance
ICE	integrated-control enablers
IDC	information dominance corps
IIA	inform and influence activities
INFOSEC	information security
IO	information operations
IOD	Information Operations Division
IP	information professionals
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
IW	Information warfare (this term is discontinued in the U.S. since but still recognized and used in commercial and military circles)
JFC	joint force commander
JFCC	joint functional component command
JFCC-GS	Joint Functional Component Command for Global Strike
JFCC-IMD	Joint Functional Component Command for Integrated Missile Defense
JFCC-ISR	Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance
JFCC-Space	Joint Functional Component Command for Space

JFCOM	Joint Forces Command
JIOC	joint information operations center
JIOWC	joint information operations warfare center
JIOWC	Joint Information Operations Warfare Center
JIOWC	Joint Information Operations Warfare Center
JP	joint publication
JSOC	Joint Special Operations Command
JTF	joint task force
JWAC	Joint Warfare Analysis Center
MAGTF	Marine Air-Ground Task Force—(U.S. Marine Corps Warfare Publication, MCWP 3–40.4, MAGTF Information Operations)
MARFORCYBER	Marine Forces Cyber Command
MARFORSTRAT	Marine Corps Forces U.S. Strategic Command
MARSOC	Marine Special Operations Command
MASINT	measurement and signature intelligence
MC WfF	mission-command warfighting function—(U.S. Army Field Manual 6–0, Mission Command, June 2011)
MCIOC	Marine Corps Information Operations Command
MCIOP	Marine Corps Information Operations Program
MCWP	Marine Corps Warfare Publication
MILDEC	military deception
MISD	Military Information Support Division
MISO	Military Information Support Operations
NetA	network attack
NetD	network defense

NetOps	network operations
NII	national information infrastructure
NS	network warfare support
NSWC	Naval Special Warfare Command
NW Ops	network-warfare operations
OOTW	operations other than war
OPLAN	operation plan
OPNAV	Office of the Chief of Naval Operations
OPORD	operation order
OPSEC	operations security
OPT	operational planning team
PA	public affairs
PBA	predictive battlespace awareness
PD	public diplomacy
PNT	precision navigation and timing
PSYOP	psychological operations
R&D	research and development
SAC	Strategic Air Command
SAD	Special Actions Division
SC	strategic communication
SCC-WMD	USSTRATCOM Center for Combating Weapons of Mass Destruction
SecDef	U.S. Secretary of Defense
SIGINT	signal intelligence
SME	subject-matter experts

SOF	special-operations forces
T&E	test and evaluation
TA	target audience
U.S.	The United States
UCP	Unified Command Plan
USA	United States Army
USAF	United States Air Force
USAFRICOM	United States Africa Command
USASOC	United States Army Special Operations Command
USCENTCOM	United States Central Command
USD(P)	Under Secretary of Defense for Policy
USEUCOM	United States European Command
USMC	United States Marine Corps
USN	United States Navy
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States Southern Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command

## **ACKNOWLEDGMENTS**

First and foremost, I am grateful to the Almighty for enabling me to pursue and complete higher education in a reputable institution. I am thankful to my service, Pakistan Navy, for having confidence in my abilities and selecting me for the postgraduate studies. My gratitude will not be complete without mentioning the United States government for providing international military officers an opportunity to excel in their careers by undergoing advanced studies in a prestigious institution like Naval Postgraduate School in Monterey. I also want to thank here the entire faculty of my curriculum for providing guidance and stimulus in their respective academic fields. I am especially grateful to my thoroughly professional advisors, Professor Steven Iatrou and Professor Edward Fisher, for their time, expertise and advise that aptly steered this thesis. A special mention of my program officer, CDR Jim Robinette, who sincerely took care of all curriculum requirements and extended all possible assistance in line with finest service traditions.

In the end, I am thankful to my parents because whatever I have achieved throughout my life is the result of their earnest supplications for my success. I am also indebted to my wife, Gullbina, for giving devoted attention to our son, Huzaifa, and daughters, Fakaiha and Farwa, whenever I was in seclusion for study. Her selfless policy of prioritizing my routine over hers afforded me an environment conducive for academic studies.

THIS PAGE INTENTIONALLY LEFT BLANK



## I. INTRODUCTION

*In the practical art of war, the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good. So, too, it is better to recapture an army entire than to destroy it, to capture a regiment, a detachment or a company entire than to destroy them. Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting.*

Sun Tzu<sup>1</sup>

### A. FOREWORD

"Information warfare" (IW) is a very broad term and much has been written about it from the military and commercial perspectives. The term is directly linked with the word "information" itself. It is a well-established fact that in today's high-tech world, a capability to acquire, leverage, and protect information and information-processing systems is compulsory for nations that wish to remain competitive in the battlefields of commerce and the military.

IW has become highly relevant in the post–Cold War era, in which the nature of conflict has been transformed from bipolar global structures to multisided local and regional contests in which the military element is a crucial part of, but not the driving force for, competition and conflict. IW as a concept covers an expanse ranging from media wars to electronic combat and from economic competition to strategic conflict waged against civilian populations. For military planners, it is important to understand the basic tenets contained within IW in order to organize its structure and train personnel accordingly.

The United States Department of Defense (DoD) has been aggressively formulating doctrine and policy on the subject since the early 1990s. Various amendments and updates, both conceptual and methodical, have been introduced into doctrine to keep this form of warfare abreast with continually changing trends. The study of this evolution offers guidelines to other coalition

---

<sup>1</sup> Samuel B. Griffith, *Sun Tzu: The art of War* (London: Oxford University Press, 1963), 41.

partners who may wish to make their own organizations effective and viable by incorporating changes to suit their scale and scope of operations.

## **B. PURPOSE**

The 1991 Gulf War (Operation Desert Storm) can be regarded as the first example in which U.S. military forces displayed their strength and skill with modern precision-guided weapons, brought to the world in real time or near real time through modern communications means.<sup>2</sup> The reason that people around the globe still remember the liberation of Kuwait is that it was a showcase of the modern face of war. Modern communication systems and networks not only assisted soldiers in the battlefield, but were also telecasting real-time scenes to millions of television viewers. This was the first major glimpse of the new digital nature of information, heralding the revolution in information technology (IT).

In 2003, the Second Gulf War (Operation Iraqi Freedom) further reinforced the importance of modern technology in maintaining communication links both with and within the battle zone. The United States today is not only a leader in IT, but also possesses the most recent combat experience of warfare fought in the era of the information revolution. Their present-day doctrine on the subject of IW, now referred to as information operations (IO), reflects painstaking research and conceptual innovation, spanning almost a quarter of a century.

For military commanders, it is often a better approach to learn from contemporary evolutionary trends in the application of warfare than to look for revolutionary ideas. Following this approach, the purpose of this thesis is to explore information warfare in light of the evolution of U.S. methodologies and to draw pertinent lessons for smaller militaries.

---

<sup>2</sup> Group Captain Sultan M Hali, "The role of media in war," *Defence Journal* .(2000), accessed June 5, 2012. <http://www.defencejournal.com/2000/aug/role-media-war.htm>

### C. THE NATURE OF INFORMATION WARFARE

Information warfare, in its most fundamental sense, is the emerging warfare area in which future nation-against-nation conflict at the strategic level is most likely to occur. IW is also changing the way operational and tactical-level combat and military activities are being planned and executed. Interestingly, IW may result in “operations other than war” being conducted, especially as it may permit a country to achieve important national-security objectives without the need for forward deployment of military forces.<sup>3</sup>

According to Toffler and Schwartz,<sup>4</sup> IW makes it possible to impose our will on the enemy by controlling, manipulating, or by prohibiting access to information. Therefore, IW may define future warfare and may be the central focus in the future of any conflict. Information systems were previously second in importance to conventional or kinetic weapons such as aircraft, tanks, ships and missiles, but today they are so critical to military operations that it may be more effective to attack an opponent’s information system than to destroy his weapons platforms. Moreover, all latest weapons and their platforms are information-intensified as their operations are dependent on information systems. These dependencies are going to make information acquisition a key objective for today’s military forces.

Warfare has historically been the domain of nation-states, or, at least, groups of displaced people fighting an oppressive government. Now, even small, loosely organized groups and individuals can conduct information warfare on an array of targets. When reviewing the military’s treatment of information as a weapon, it is important to note that IW is much more than using information to aid conventional destruction. Warfare is gradually losing its material nature, and

---

<sup>3</sup> Air Marshal Raghu Rajan, “Impact of Information Warfare on Aerospace Operations,” *IDR* Issue Vol 26.2 Apr-Jun 2011, accessed June 4, 2012, <http://www.indiandefencereview.com/interviews/impact-of-information-warfare-on-aerospace-operation>

<sup>4</sup> Daniel Ventre, *Information Warfare* (London: ISTE Ltd, 2009), 32.

information has become an end in itself. As governments, businesses, and individuals become increasingly reliant on data storage and movement, the potential for serious economic harm resides in the information itself<sup>5</sup>. Keeping in view the increased importance of information and its processing systems, every military entity should institute a robust IW infrastructure to be able to leverage information when and where appropriate.

## **D. THESIS OVERVIEW**

### **1. Scope of the Study**

This thesis will review the literature on IW. A description of frequently used lexicon and terminology will be presented to clarify ambiguities associated with the theory of IW. Fundamental concepts and definitions from U.S. publications will be briefly discussed. Based on this study, an approach to organizing IW forces that is feasible for smaller regional militaries will be suggested.

### **2. Thesis Organization**

The remainder of this thesis follows the chapter outline below:

Chapter II provides a historical background on information warfare and its distinction from information operations. The thesis clarifies the relationship between information warfare and other current terminologies, such as command-and-control warfare (C2W), information campaigns, and perception management.

Chapter III explains the United States DoD interpretation and metamorphous of the term “information warfare” and its related capabilities and characteristics.

Chapter IV looks into the way the U.S. DoD and armed forces have implemented IO across their departments. Since the present model has evolved over a period of approximately twenty years, a grassroots examination is made

---

<sup>5</sup> Carter Gilmer, “The Future of Information Warfare,” SANS Institute (2001) GSEC Practical Assignment Version 1.2f

by this study. This chapter also looks at tactical, operational, and strategic requirements that have forced a number of conceptual and doctrinal changes in IW.

Chapter V presents guidelines for developing nations that are useful for implementing IW in their policy and strategy planning and execution. A simple model is presented that illustrates the promise of IW capabilities in the modern era.

Chapter VI presents summary of the study, provides recommendations for establishing an effective IW capability, and concludes the thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

## II. CONCEPTUAL UNDERSTANDING OF THE TERM “IW”

### A. SCOPE/DIMENSIONS OF IW

The vast scope of information warfare is clearly demonstrated by the following comments by Edwin Leigh Armistead<sup>6</sup>:

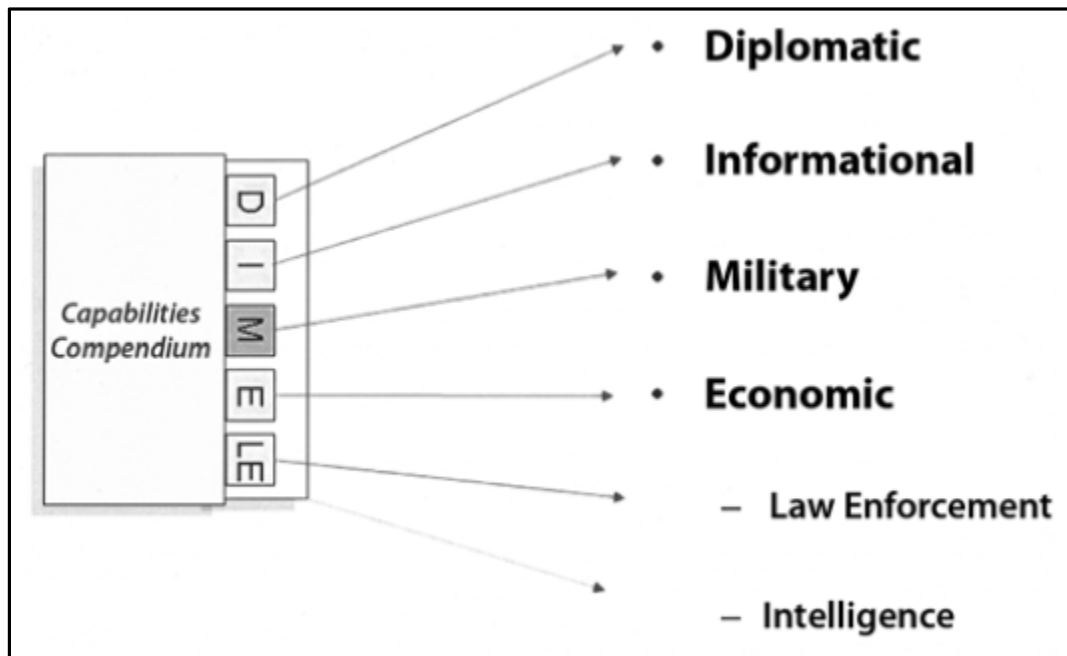
The Information Age is an era of manipulated images, both visual and auditory. Nations, groups and individuals are all attempting to manage the message that you see, and they will often conduct their information campaign in a similar manner—whether they are ‘selling’ a soft drink or a global terrorist threat. The whole idea is to influence the ‘wetware’ of the consumer or the public, to get them to believe in a product or cause. The process is to supply information that molds the recipient’s knowledge and expectations which then results in behavior meeting the goals of the information sender.

IW deals with information and information systems; hence, its scope is not solely limited to the military sphere of application. This, at first glance, does not appear to conform with the U.S. approach to information operations (since the term “IW” no longer appears in U.S. doctrine and is replaced with “IO”). Under this approach, warfare capabilities and tools should not be applied to neutral or friendly populations or domestic audiences outside a combat zone, during a state of peace or conflict. Abandoning the term “IW” in favor of “IO” provides the flexibility and leverage of including capabilities like public affairs (PA) and defense support to public diplomacy (DSPD) to dovetail with other elements of IO. It is important to note here that, per the latest definition in *Joint Publication 1–02*, IO falls under the “military” element of national power among the four recognized elements known commonly as DIME: diplomatic, informational, military, and economic power, as shown in Figure 1. From this standpoint, the

---

<sup>6</sup> Edwin Leigh Armistead and Thomas Murphy, “The Evolution of Information Operations Contracts across the DoD: Growth Opportunities for Academic Research” (Proceedings of the 2<sup>nd</sup> International Conference on Information Warfare and Security, 8–9 March 2007).

term “IO” (or “IW” for those outside the U.S. who may use the term) cannot be used outside the sphere of military operations; this seriously limits the scope and potential that IO offers.



*Note: The national elements of power are typically recognized in the U.S. as diplomatic, informational, military and economic. Many writers include law enforcement and intelligence capabilities in the lineup. However, national security strategy reflects the first four only.*

Figure 1. National Elements of Power<sup>7</sup>

The importance of applying IO over a broader scheme of operations is evident in the following excerpt from U.S. Congressman Rob Simmons:

I see IO as the foundation for revitalizing our national power and our national prosperity. I see IO as central to both our effectiveness overseas in projecting American values and protecting American interests, and I see IO as central to our homeland defense in as much as it helps to educate our citizens about global realities, and

---

<sup>7</sup> Richard J. Josten, “Strategic Communication: Key Enabler for Elements of National Power,” IOSPHERE (Joint Information Operations Center), Summer 2006. Accessed November 2, 2012. [http://www.carlisle.army.mil/DIME/documents/iosphere\\_summer06\\_josten.pdf](http://www.carlisle.army.mil/DIME/documents/iosphere_summer06_josten.pdf)



helps our citizens to communicate bottom-up dots through Community Intelligence Centers and networks.<sup>8</sup>

In a general sense, the desire for dominance in the commercial/corporate sector, whether on an international scale or dealing only with domestic competition within a country, can shape IW into many forms, as driven by “ends, ways, and means.”<sup>9</sup> At a strategic level, IW can be waged, for example, against a hostile nation to ruin its national economy. This mode of attack may prove more devastating and damaging than otherwise possible through the employment of conventional military forces. Similarly, grievances or deprivations may motivate a group of antagonists to initiate a campaign against a government with the help of few personal computers. IW is available to hackers who can target across borders against any organization, at their discretion. Thus, in order to understand IW, a brief look from the civil and military perspectives is helpful.

## **B. NON-MILITARY/CIVIL PERSPECTIVE OF IW**

The proper development of IW capability can support policies, processes and strategies of traditional hierarchical militaries and governments, as well as business organizations and their growth. On one hand, IW is getting increasingly involved in management and operational issues involving combat activities; on the other, it is being utilized and modeled to address any large-scale, complex organization and its mission. This is because the general requirements for

---

<sup>8</sup> Rob Simmons, “*Information Operations: All Information, All Languages, All the Time.*” Accessed on November 02, 2012.  
[http://www.google.com/url?sa=t&rct=j&q=is%20io%20part%20of%20dime&source=web&cd=5&cad=rja&ved=0CDIQFjAE&url=http%3A%2F%2Fwww.oss.net%2Fdynamaster%2Ffile\\_archive%2F051109%2Faf481ac312ef876d0fab0965a09b28df%2F004%2520Body%2520of%2520Book%2520with%2520Footnotes.doc&ei=mxUUL-wOaG4igLb3oGQDg&usg=AFQjCNHU9\\_Cg8lby-tyBLjEbLSVJMeM\\_uw](http://www.google.com/url?sa=t&rct=j&q=is%20io%20part%20of%20dime&source=web&cd=5&cad=rja&ved=0CDIQFjAE&url=http%3A%2F%2Fwww.oss.net%2Fdynamaster%2Ffile_archive%2F051109%2Faf481ac312ef876d0fab0965a09b28df%2F004%2520Body%2520of%2520Book%2520with%2520Footnotes.doc&ei=mxUUL-wOaG4igLb3oGQDg&usg=AFQjCNHU9_Cg8lby-tyBLjEbLSVJMeM_uw)

<sup>9</sup> Clausewitz described the relationship of ends, ways, and means in terms of a “paradoxical trinity” which has been interpreted as the government, military, and people. The government is responsible for defining the desired political environment at the conclusion of conflict (the ends), the military is primarily responsible for developing the strategy (the ways), and the people, as represented by Congress, provide the will and resources (the means). This excerpt is taken from, Bruce J. Reider, “Strategic Realignment: Ends, Ways, And Means In Iraq,” the U.S. Army professional writing collection. Accessed on November 2, 2012.  
[http://www.army.mil/professionalwriting/volumes/volume6/february\\_2008/2\\_08\\_3.html](http://www.army.mil/professionalwriting/volumes/volume6/february_2008/2_08_3.html)

success are often very similar for a defense force or a business, giving information warfare a broader application beyond typical military-combat operations<sup>10</sup>.

The IW methodology normally adopted in the civilian sector is mainly dependent upon the target audience<sup>11</sup>. Based on the target audience, IW falls into three classifications:<sup>12</sup>:

### **1. Personal Information Warfare**

This is known as Class I information warfare and is aimed against individual privacy, involving attacks on personal and confidential data.

### **2. Commercial Information Warfare:**

This is known as Class II information warfare and involves industrial espionage and broadcasting of false information against business rivals using the Internet.

### **3. Global Information Warfare**

This is known as Class III information warfare and is aimed at countries, political alliances and spheres of influence, global economic forces, sensitive national information systems and infrastructure.”

## **C. THE MILITARY PERSPECTIVE OF IW**

### **1. Distinguishing IW from IO**

The terms “information warfare” and “information operations” are frequently used together without discretion and are normally considered interchangeable. To some people, “information warfare” is a generic term that

---

<sup>10</sup> Armistead and Murphy, op. cit.

<sup>11</sup> Target audience (also called TA) is defined by *U.S. Joint Publication 1–02* as an individual or group selected for influence.

<sup>12</sup> Amit Grover, “Cyber War’s Final Frontier: Network Centric Warfare Framework,” accessed June 25, 2012, [http://www.itffroc.org/articles/ag\\_cyberwar.pdf](http://www.itffroc.org/articles/ag_cyberwar.pdf)

represents all forms of struggle for control and superiority concerning information. This perception or impression emanates from the literal meaning of the term “information warfare.” In the context of military applications, these terms have been defined with a clear description of purpose and capabilities to facilitate proper planning, training, and execution. It is important for the practitioner of information and information systems to understand both terms conceptually without confusion.

From the available literature, it is evident that “information warfare” is the older of the two terms, emerging in the late 1970s with command and control warfare (C2W) as war-fighting constructs integrating several diverse capabilities. These further evolved into “information operations,” recognizing the role of information as an element of power across the spectrum of peace, conflict, and war<sup>13</sup>.

In the United States, “information operations” is the superior strategic term, integrating various capabilities and activities such as information warfare<sup>14</sup>. Though the definition of IO has undergone many revisions and updates to date, a 1998 JP 3–13 defined it in a very broad sense. Per this publication, information operations involve actions taken to affect adversary information and information systems while defending one’s own information and information systems. In the same year, information warfare was viewed as an extension of an overall IO effort pitched specifically when a state of peace is no longer present between or among countries. Information warfare was defined as information operations conducted during times of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries.<sup>15</sup> The latest definition of IO specifically associates it with military operations only (no civil

---

<sup>13</sup> U.S. Army War College Information Operations Primer November 2011

<sup>14</sup> Manuel W. Wik, “Revolution in Information Affairs,” *Tactical and Strategic Implications of Information Warfare and Information Operations*: 14, accessed on July 3, 2012, doi: 10.1.1.196

<sup>15</sup> JP 3–13, Joint Doctrine for Information Operations (Washington, DC: U.S. GPO, 9 October 1998): I-1

interpretation or application) and lays more emphasis on integration, synchronization, and coordination of various information-related capabilities. “The ultimate goal of information operations is to impact human decision making. Ultimately, it could be the struggle of minds in order to become the master of a situation.”<sup>16</sup>

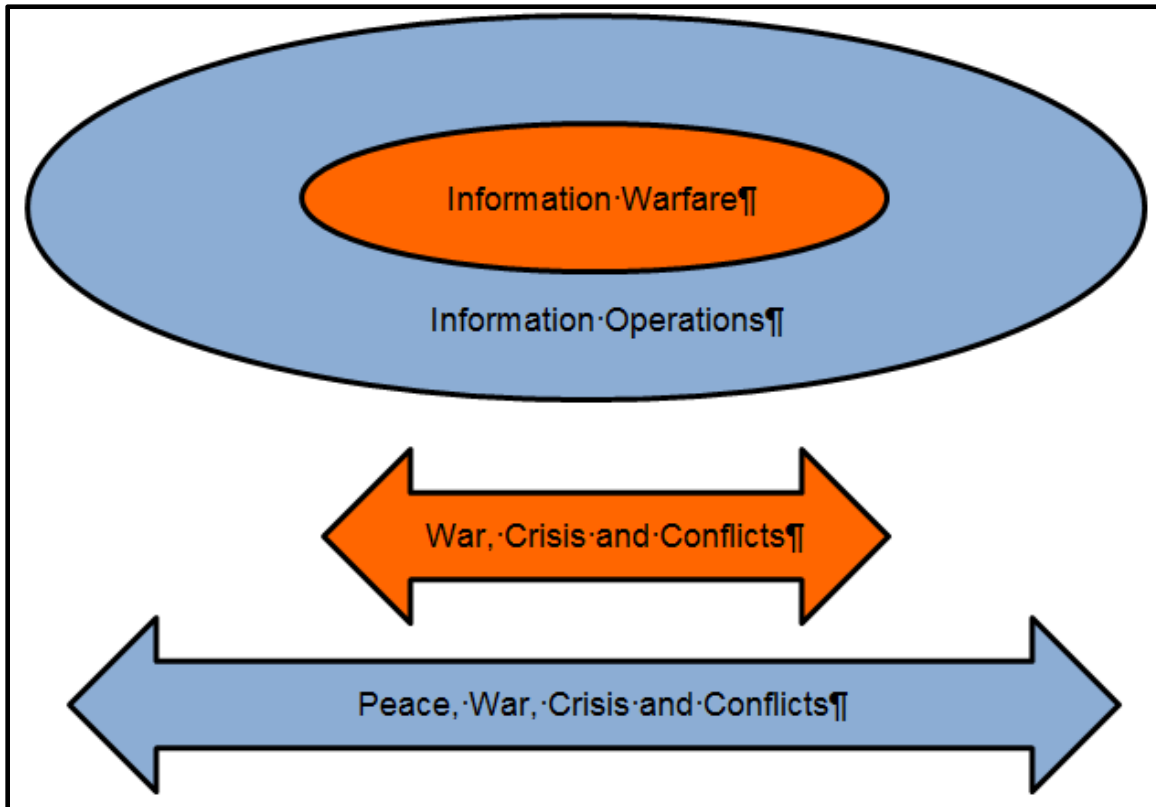


Figure 2. Differences in scope between IW and IO

It is relevant to review the range of military operations to better understand the ongoing discussion of the applicability of IW and IO across different states. The following table is helpful in understanding the spectrum of environments in which military operations may occur.

---

<sup>16</sup> Manuel W. Wik, “Revolution in Information Affairs,” *Tactical and Strategic Implications of Information Warfare and Information Operations*: 14, accessed on July 3, 2012, doi: 10.1.1.196

STATES OF THE ENVIRONMENT	GOAL	MILITARY OPERATIONS	TYPE		EXAMPLES
War	Fight and Win	War	C o m b a t	N o n c o m b a t	<ul style="list-style-type: none"><li>• Large-scale combat operations</li><li>• Attack</li><li>• Defend</li></ul>
Conflict	Deter War and Resolve Conflict	Operations other than war			<ul style="list-style-type: none"><li>• Strikes and raid</li><li>• Peace enforcement</li><li>• Support to insurgents</li><li>• Antiterrorism</li><li>• Peacekeeping</li><li>• Noncombatant evacuation operations (NEO)</li></ul>
Peacetime	Promote Peace	Operations other than war			<ul style="list-style-type: none"><li>• Counter-drug</li><li>• Disaster relief</li><li>• Civil support</li><li>• Peace building</li><li>• Nation assistance</li></ul>
Note: The states of peacetime, conflict and war could all exist at once in the theater commander's strategic environment. He can respond to requirements with a wide range of military operations. Noncombat operations might occur during war, just as some military operations other than war (MOOTW) might require combat.					

Table 1. The Range of Military Operations<sup>17</sup>

From this discussion, it is evident that the realm of information operations is much larger than information warfare. From the standpoint that the ultimate goal of operations in the military is its ability to contribute to the traditional military

<sup>17</sup> U.S. Army Field Manual (FM) 100-7, *Decisive Force: The Army in Theater Operations*, Headquarters Department of the Army Washington, DC, 31 May 1995: 2-2

mission of fighting and winning the nation's wars, information operations connect ultimately to information warfare. However, it is pertinent to note that the U.S. DoD has officially discontinued the use of term "information warfare" and removed it from joint IO doctrine and related publications<sup>18</sup>. Today, information operations deal exclusively with all the attributes information may have, whether in peacetime or hostilities. Generally, peace operations nowadays are becoming part and parcel of a military's charter of duties on a global level. In these "operations other than war" (OOTW), information operations are increasingly finding an important role to play in enhancing the success rate of such missions.

## **2. The Targets of Information Warfare<sup>19</sup>**

In an information environment,<sup>20</sup> humans and information infrastructure are both prime targets of IW. The widely used term information infrastructure refers to the complex of sensing, communicating, storing, and computing elements that comprise a defined information network conveying analog and digital voice, data, imagery, and multimedia data. The "complex" includes the physical facilities (computers, links, relays, and node devices), network standards and protocols, applications and software, the personnel who maintain the infrastructure, and the information itself. The infrastructure is the object of both attack and defense; it provides the delivery vehicle for the information weapons of the attacker while forming the warning net and barrier of defense for the defender. Understanding of the physical and abstract structure of the infrastructure is therefore essential for both the defender and the target alike.

Three infrastructure categories are most commonly identified.

- The global information infrastructure (GII) includes the international complex of broadcast communications, telecommunications, and

---

<sup>18</sup> U.S.JP 3–13, Information Operations (Washington, DC: U.S. GPO, 13 February 2006): iii

<sup>19</sup> Information in this section is taken from Edward Waltz, *Information Warfare Principles and Operations* (Norwood: Artech House, 1998), 173–174.

<sup>20</sup> Information environment is defined in U.S. JP 1–02as 'the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information'.

computers that provide global communications, commerce, media, navigation, and network services between NIIs.

- The national information infrastructure (NII) includes the subset of the GII within the nation, and internal telecommunications, computers, intranets, and other information services not connected to the GII. The NII is directly dependent upon national electrical power to operate, and the electrical power grid is controlled by components of the NII. The GII can be described as the interconnection layer between NIIs.
- The defense information infrastructure (DII) includes the infrastructure owned and maintained by the military (and intelligence) organizations of the nation for purposes of national security. The DII includes command, control, communications, and computation components as well as dedicated administration elements. These elements are increasingly integrated to the NII and GII to use commercial services for global reach but employ information security (INFOSEC) methods to provide appropriate levels of security.

#### **D. INFORMATION CAMPAIGN IN INFORMATION OPERATIONS VIS-A-VIS PERCEPTION MANAGEMENT**

“Information campaign”<sup>21</sup> is a term frequently used in the military and commercial worlds. It is pertinent to describe its conceptual description and relevance to information operations, and how it differs from perception management. There is no proper definition of this terminology in U.S. DoD publications, but since its use is common in print and electronic media, its proper context should be clear to military personnel. In addition, the distinction between perception management and an IO information campaign is not readily apparent, and boundaries between these terminologies seem to be blurring.

*Joint Publication 1–02, Department of Defense Dictionary of Military and Associated Terms*, defines perception management as:

... actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and

---

<sup>21</sup> JP 1–02 defines campaign as a series of related major operations aimed at achieving strategic and operational objectives within a given time and space.

leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations.<sup>22</sup>

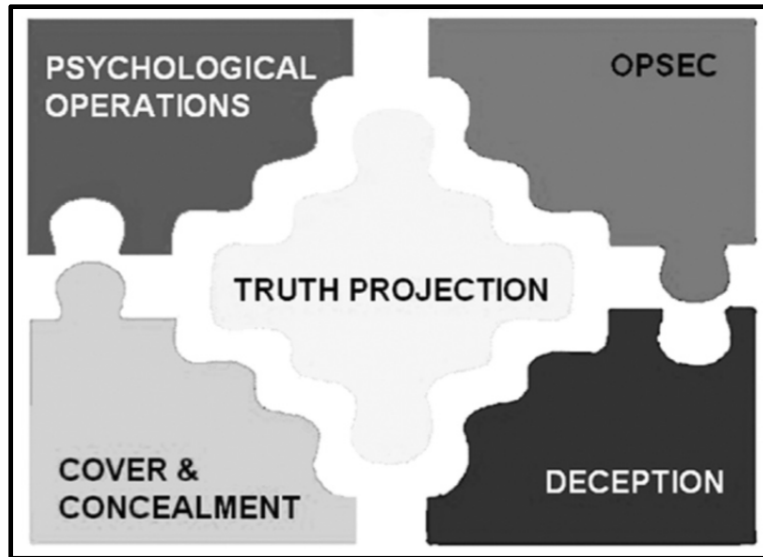


Figure 3. Perception management<sup>23</sup>

As a matter of concept, information campaigns are an important technique employed in information operations where the intent is to disseminate true and unclassified information about military operations and create a reliable information environment for external audiences. Such an effort is extremely helpful in countering propaganda and disinformation generated by foreign governments and factions that control or intimidate the media and try to distort the overall picture. On the other hand, perception management allows the use of falsehood and deception (as part of its definition) where the purpose is to get the other side to believe what one wishes it to believe, whatever the truth may be.

---

<sup>22</sup> Joint Chiefs of Staff (JCS) Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms (Washington, DC: U.S. GPO, 12 April 2001, as amended through 13 June 2007) page 407.

<sup>23</sup> Lieutenant Colonel Garry J. Beavers, U.S. Army, Retired, "Defining the Information Campaign," *Military Review* November-December 2005: 80



Potentially all IO capabilities, including, but not limited to, PA, PSYOPs, and counterpropaganda, can contribute to an information campaign. Information assurance figures in the mix by protecting and defending information and information systems. As part of an information campaign, OPSEC would identify, control, and protect unclassified evidence associated with sensitive operations and activities.<sup>24</sup> These components are shown in mosaic form in Figure 4.

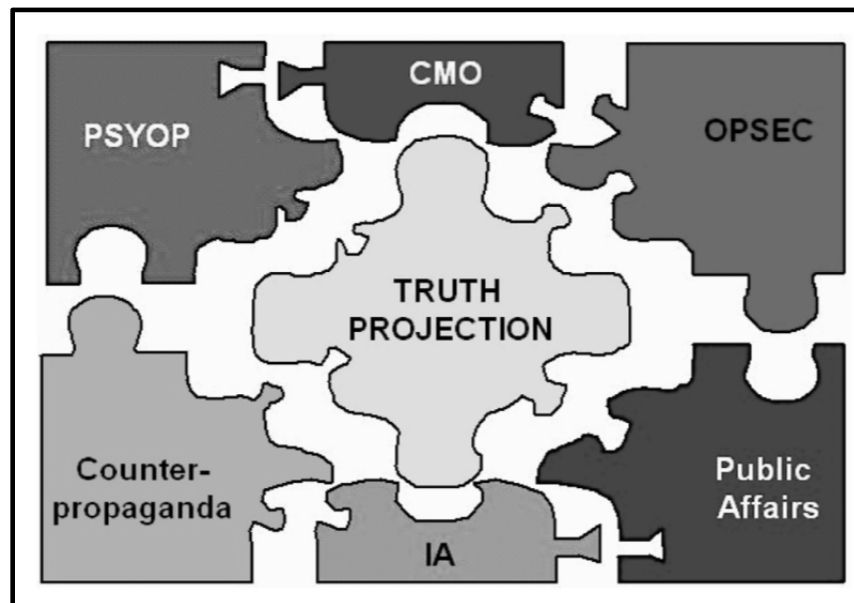


Figure 4. Components of an information campaign<sup>25</sup>

Information campaigns have played a significant role throughout history in the fulfillment of military objectives at strategic and operational levels of warfare. Their future role will potentially increase and extend to tactical forces. Modern warfare banks heavily on influencing audiences both internal and external. In today's world, where scores of information channels and networks are readily available to target audiences, deception and perception-shaping efforts, without

---

<sup>24</sup> Ibid., 82

<sup>25</sup> Ibid., 81

careful consideration, planning, and coordination, can be futile and even risky. Hence, detailed planning and coordination are of paramount importance in every information campaign.

### **III. U.S. JOINT AND SERVICES LEVEL INTERPRETATION OF INFORMATION OPERATIONS**

#### **A. INTRODUCTION**

As described earlier, the U.S. DoD has carried out extensive research and doctrinal work in the field of IO and information-related capabilities. That effort is still ongoing, with continual revisions and modifications of the literature and updating of the organizational framework for implementing IO. A study of U.S. DoD publications on the subject of, or relating to, IO provides not only the insight on the evolutionary process in this field, but also gives the extent and depth of possible avenues that might play a role in warfare within the information realm.

#### **B. JOINT FORCES COMMAND PERSPECTIVE ON IO**

##### **1. Important Terminology Used in IO Literature**

Before venturing into the definition of IO, it is important to understand some important operational terminologies often encountered in IO literature. Operations are often characterized by using terms such as domains, environment, effects, targets, and capabilities.

Our universe consists of three primary dimensions: physical (including the terrestrial, atmospheric, marine, space, and electromagnetic environments, as well as the tangible components contained within them), cognitive (the single and collective consciousness that exists in the minds of individuals), and informational (existing within both the physical and cognitive dimensions and hosting the creation, manipulation, storage, and sharing of data, and containing the information itself).<sup>26</sup> This last dimension actually links the physical real world with the human consciousness of the cognitive dimension, both as a source of input (stimulus, senses, etc.) and to convey output (intent, direction, decisions, etc.).<sup>27</sup>

---

<sup>26</sup> Timothy P. Franz, Matthew F. Durkin, Paul D. Williams, Richard A. Raines, Robert F. Mills, *Defining Information Operations Forces*, Air & Space Power Journal Summer 2007: 54.

<sup>27</sup> *Information Operations Primer*, U.S. Army War College, November 2011.

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.<sup>28</sup> Due to the inherent nature of the information environment, it exists in and extends to all interrelated physical, informational, and cognitive dimensions. Similarly, the information environment pervades and transcends the boundaries of physical dimensions (i.e., land, sea, air, and space domains) and encompasses cyberspace in itself. This environment is of particular importance in IO, as a variety of capabilities is employed to impact the above-mentioned three dimensions, partially or fully.

An operational domain represents a portion of one or more primary domains chosen for a specific national or military operation. Essentially, it is an artificially defined (in that it is defined by humans), bounded area of the universe. A pertinent example is cyberspace. The cyberspace operational domain is “characterized by the use of electronics and the electromagnetic environment to store, modify, and exchange data and information via networked systems and associated physical infrastructure.”<sup>29</sup> Per U.S. joint publication (JP) 1–02, cyberspace is defined as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers”<sup>30</sup>. Within any operational domain, *capabilities* achieve *effects* against specific *targets*.<sup>31</sup> Leveraging joint doctrine, we define a *target* as “an entity or object considered for possible engagement or other action.”<sup>32</sup> Using the same reference, we define an *effect* as

---

<sup>28</sup> Joint Publication (JP) 1–02, Department of Defense Dictionary of Military and Associated Terms (Washington, DC: U.S. GPO, 8 November 2010, as amended through 15 July 2012): 152.

<sup>29</sup> Franz op. cit., 54–55.

<sup>30</sup> Joint Publication (JP) 1–02, Department of Defense Dictionary of Military and Associated Terms (Washington, DC: U.S. GPO, 8 November 2010, as amended through 15 July 2012): 80.

<sup>31</sup> Franz op. cit., 54–55.

<sup>32</sup> Joint Publication (JP) 1–02, Department of Defense Dictionary of Military and Associated Terms (Washington, DC: U.S. GPO, 8 November 2010, as amended through 15 July 2012): 310.

“the physical or behavioral state of a system that results from an action, a set of actions, or another effect. Effect can also be a change to a condition, behavior, or degree of freedom.”<sup>33</sup> Finally, we draw upon the DoD directive to define *capabilities* as “the ability to achieve a desired effect under specified standards and conditions through a combination of means and ways across doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) to perform a set of tasks to execute a specified course of action.”<sup>34</sup>

## **2. Defining IO**

In a recently amended *JP 1–02*, IO is defined as “the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.”<sup>35</sup> This definition was introduced in a U.S. Secretary of Defense memorandum issued on January 25, 2011.

This definition represents a marked shift in the approach toward IO. It is now regarded more as a combination of capabilities, individual and diverse in nature, that are required to be employed together in a coherent manner under the umbrella of IO. Per the latest instructions, it is not practical to label or tag any particular capability or set of capabilities as belonging exclusively to IO like a proprietary feature. IO has been introduced this time as more of an integrating function, more emphatically and explicitly than ever before. The new policy also

---

<sup>33</sup> Joint Publication (JP) 1–02, Department of Defense Dictionary of Military and Associated Terms (Washington, DC: U.S. GPO, 8 November 2010, as amended through 15 July 2012): 101.

<sup>34</sup> Department of Defense Directive (DODD) number 7045.20, *Capability Portfolio Management*, September 25, 2008: 8.

<sup>35</sup> Joint Publication (JP) 1–02, Department of Defense Dictionary of Military and Associated Terms (Washington, DC: U.S. GPO, 8 November 2010, as amended through 15 July 2012): 152.

focuses on the distribution of the oversight responsibility of the core capabilities among various entities in order to better address the issues of management, funding, training and resources.

To appreciate the notable differences in the new definition as compared to older versions, it is logical to restate the previous definitions. In the 2006 edition, *JP 3–13* described IO as “the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.”<sup>36</sup> In an even earlier 1998 edition of *JP 3–13*, IO was defined as “actions taken to affect adversary information and information systems while defending one’s own information and information systems.”<sup>37</sup> It may be noted here that the latest definition is an improved and modified description of the same idea introduced in this 1998 definition. The new definition recognizes employment of IO tools and resources in military operations only and limits its use to the military only. Moreover, like the 1998 definition, the new approach recognizes the fact that an IO operation may not require all of the capabilities to be put in or brought together to achieve success. The selection of the capabilities is situation dependent and to be determined by the military commander according to his or her appreciation of the need and situation. At times a single, or few, capabilities can be sufficient to fulfill the objective, and any attempt to be more inclusive can ruin the outcome instead.

### **C. CAPABILITIES INVOLVED IN IO**

As highlighted earlier, information operations are the right combination of various capabilities according to the dictates of the information environment.

---

<sup>36</sup> JP 3–13, Information Operations (Washington, DC: U.S. GPO, 13 February 2006): I-1.

<sup>37</sup> JP 3–13, Joint Doctrine for Information Operations (Washington, DC: U.S. GPO, 9 October 1998): GL-7.

Some capabilities have been in existence and use since the dawn of warfare; others are the result of technological innovations and advancements. The U.S. DoD described these capabilities as core, supporting, and related, based on their relative importance in achieving the supreme objective of affecting the decision-making capability of the adversary (an overview of these capabilities is shown in Figure 5). It is due to this nature of information operations that synchronization and coordination become the most important attribute of planning and execution. The following is a general description of these capabilities.

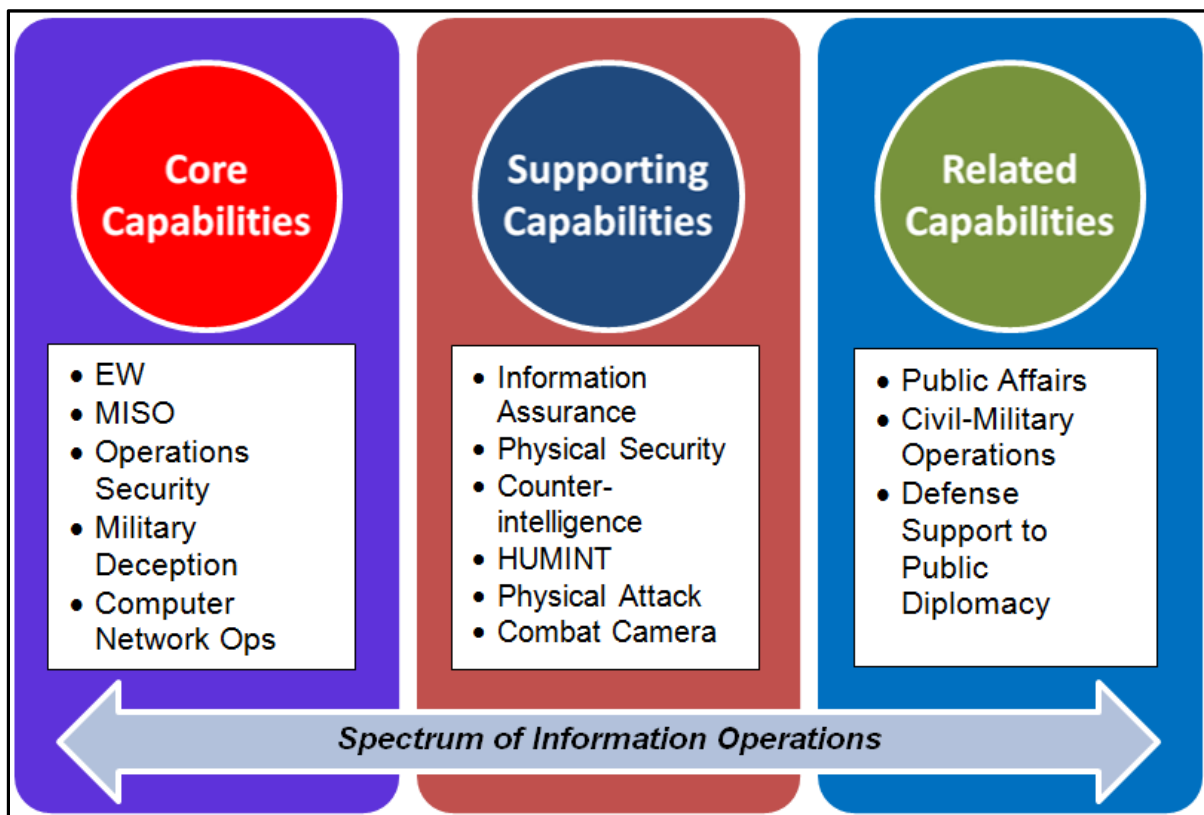


Figure 5. Capabilities involved in IO

### 1. Core Capabilities

IO as defined in the 2006 joint publication consists of five core capabilities: military information support operations (MISO, previously known as psychological

operations or PSYOPs<sup>38</sup>), military deception (MILDEC), operations security (OPSEC), electronic warfare (EW), and computer-network operations (CNO, now commonly referred to as cyber). Of the five, PSYOPs/ MISO, OPSEC, and MILDEC have played a major part in military operations for many centuries. In this modern age, they have been joined first by EW and most recently by CNO/Cyber. Together, these five capabilities, used in conjunction with supporting and related capabilities, provide the JFC with the principal means of influencing an adversary and other target audiences (TAs) by enabling the joint forces freedom of operation in the information environment.<sup>39</sup>

## **2. Supporting Capabilities**

Capabilities supporting IO include information assurance (IA), physical security, physical attack, counterintelligence (CI), human intelligence (HUMINT)<sup>40</sup> and combat camera (COMCAM). These are either directly or indirectly involved in the information environment and contribute to effective IO. They should be integrated and coordinated with the core capabilities, but can also serve other wider purposes.<sup>41</sup>

## **3. Related Capabilities**

There are three military functions specified as related capabilities for IO: public affairs (PA), civil–military operations (CMO), and defense support to public diplomacy (DSPD). These capabilities make significant contributions related to IO and must always be coordinated and integrated with the core and supporting information operations capabilities. However, their primary purpose and rules

---

<sup>38</sup> The definition included in JP 3–13 (published 13 February 2006) has been superseded by the U.S. SecDef Memo 12401–10 (25 January 2011). The term psychological operations (PSYOP) has been replaced by military information support operations (MISO).

<sup>39</sup> JP 3–13, Information Operations (Washington, DC: U.S. GPO, 13 February 2006): II-1.

<sup>40</sup> HUMINT has been added in supporting capabilities of IO through Department of Defense Directive (DODD) 3600.01 Information Operations, 14 August 2006, Change 1 incorporated 23 May 2011.

<sup>41</sup> JP 3–13, Information Operations (Washington, DC: U.S. GPO, 13 February 2006): II-5.



under which they operate must not be compromised by IO. This requires additional care and consideration in the planning and conduct of IO. For this reason, the PA and CMO staffs, particularly, must work in close coordination with the IO planning staff.<sup>42</sup>

#### **4. Core Capabilities in IO**

##### ***a. Military Information Support Operations (MISO)***

These are planned operations to convey selected truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of their governments, organizations, groups, and individuals. The purpose of MISO is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. MISO are a vital part of the broad range of U.S. activities to influence foreign audiences and are the only DoD operations authorized to influence foreign TAs directly through the use of radio, print, and other media. MISO personnel advise the supported commander on methods to capitalize on the psychological impacts of every aspect of force employment and how to develop a strategy for developing and planning the dissemination of specific MISO programs, to achieve the overall campaign objectives.<sup>43</sup>

##### ***b. Military Deception (MILDEC)***

MILDEC is described as those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly force's mission. MILDEC and OPSEC are complementary activities—MILDEC seeks to encourage incorrect analysis, causing the adversary to arrive at specific false deductions, while OPSEC seeks to deny real information to an adversary, and

---

<sup>42</sup> Ibid., II-8.

<sup>43</sup> Ibid., II-1.

prevent correct deduction of friendly plans. To be effective, a MILDEC operation must be susceptible to adversary collection systems and “seen” as credible to the enemy commander and staff. A plausible approach to MILDEC planning is to employ a friendly course of action (COA) that can be executed by friendly forces and that adversary intelligence can verify. However, MILDEC planners must not fall into the trap of ascribing to the adversary particular attitudes, values, and reactions that “mirror image” likely friendly actions in the same situation, i.e., assuming that the adversary will respond or act in a particular manner based on how we would respond.<sup>44</sup>

**c. *Operations Security***

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions and other activities to identify what friendly information is necessary for the adversary to have sufficiently accurate knowledge of friendly forces and intentions; deny adversary decision makers critical information about friendly forces and intentions; and cause adversary decision makers to misjudge the relevance of known critical friendly information because other information about friendly forces and intentions remain secure.<sup>45</sup>

**d. *Electronic Warfare***

EW refers to any military action involving the use of electromagnetic (EM) and directed energy to control the EM spectrum or to attack the adversary. EW includes three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). EA involves the use of EM energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying adversary combat capability. EP ensures the friendly use of the EM spectrum. ES consists of actions tasked by, or under direct control of, an

---

<sup>44</sup> Ibid., II-2.

<sup>45</sup> Ibid., II-3.

operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. ES provides information required for decisions involving EW operations and other tactical actions such as threat avoidance, targeting, and homing. ES data can be used to produce SIGINT, provide targeting for electronic or other forms of attack, and produce measurement and signature intelligence (MASINT). SIGINT and MASINT can also provide battle damage assessment (BDA) and feedback on the effectiveness of the overall operational plan.<sup>46</sup>

**e. *Computer Network Operations***

CNO is one of the latest capabilities developed in support of military operations. CNO stems from the increasing use of networked computers and supporting IT infrastructure systems by military and civilian organizations. CNO, along with EW, is used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure. For the purposes of military operations, CNO are divided into computer-network attack (CNA), computer-network defense (CND), and related computer-network exploitation (CNE) enabling operations. CNA consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident on computers and computer networks, or the computers and networks themselves. CND involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. CND actions not only protect DoD systems from an external adversary, but also from exploitation from within, and are now a necessary function in all military operations. CNE is enabling operations and

---

<sup>46</sup> Ibid., II-4.

intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks<sup>47</sup>.

## **D. INFORMATION OPERATIONS SUPPORTING CAPABILITIES**

### **1. Information Assurance**

IA is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. IA is necessary to gain and maintain information superiority. IA requires a defense-in-depth approach that integrates the capabilities of people, operations, and technology to establish multilayer and multidimensional protection to ensure survivability and mission accomplishment. IA must assume that access can be gained to information and information systems from inside and outside DoD-controlled networks<sup>48</sup>.

### **2. Physical Security**

Physical security is that part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. The physical security process includes determining vulnerabilities to known threats, applying appropriate deterrent, control and denial safeguarding techniques and measures, and responding to changing conditions.<sup>49</sup>

---

<sup>47</sup> Ibid., II-5.

<sup>48</sup> Ibid., II-6.

<sup>49</sup> Ibid., II-6.

### **3. Physical Attack**

The concept of attack is fundamental to military operations. Physical attack disrupts, damages, or destroys adversary targets through destructive power. Physical attack can also be used to create or alter adversary perceptions or drive an adversary to use certain exploitable information systems.<sup>50</sup> This term has been modified in Department of Defense Directive (DODD) 3600.01 (after incorporation of change 1 on 23 May 2011) as physical (kinetic attack) that may be employed alone or integrated with non-kinetic attack options to influence or disrupt adversary decision makers or groups and provide support for full-spectrum dominance.

### **4. Counterintelligence**

CI consists of information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities.<sup>51</sup>

### **5. Human Intelligence**

HUMINT and related intelligence activities are those deriving information collected from human sources, and shall be used to support IO. For collection of information that may endanger the source or the collector, then the information shall only be collected by trained and certified HUMINT collectors who are assigned to organizations with a mission to collect HUMINT in response to validated intelligence requirements. The direction and control of HUMINT activities is an inherently governmental function and may only be performed by USG civilian or military personnel.<sup>52</sup>

---

<sup>50</sup> Ibid., II-7.

<sup>51</sup> Ibid., II-7.

<sup>52</sup> Department of Defense Directive (DODD) 3600.01 Information Operations, 14 August 2006, Change 1 incorporated 23 May 2011: 3.

## **6. Combat Camera**

The COMCAM mission is to provide the OSD, the Chairman of the Joint Chiefs of Staff (CJCS), the military departments, the combatant commands, and the joint task force (JTF) with an imagery capability in support of operational and planning requirements across the range of military operations. COMCAM is responsible for rapid development and dissemination of products that support strategic and operational IO objectives. The COMCAM program belongs to the Defense Visual Information Directorate, which falls under the Assistant Secretary of Defense for Public Affairs. When deployed, operational control of COMCAM forces can be delegated to any echelon of command at the discretion of the joint force commander (JFC) and subordinate commanders. COMCAM may be coordinated by the IO staff at the JFC, component, and subordinate unit levels. Most large JTF organizations will have a joint COMCAM management team assigned to manage COMCAM and to assist in the movement of imagery. Additionally, there are usually one or more joint or component-specific COMCAM teams assigned to the theater. These component teams may be assigned to special-operations forces (SOF) or other specific units.<sup>53</sup>

## **E. INFORMATION-OPERATIONS-RELATED CAPABILITIES**

### **1. Public Affairs**

PA are those public-information, command-information, and community-relations activities directed toward both external and internal audiences with interest in DoD. PA is essential for joint forces information superiority, and credible PA operations are necessary to support the commander's mission and maintain essential public liaisons. PA's principal focus is to inform domestic and international audiences of joint operations to support combatant command public information needs.<sup>54</sup>

---

<sup>53</sup> JP 3-13, Information Operations (Washington, DC: U.S. GPO, 13 February 2006): II-8.

<sup>54</sup> Ibid., II-8.

## **2. Civil–Military Operations**

CMO are the activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace. They are conducted across the range of military operations to address root causes of instability, assist in reconstruction after conflict or disaster, or may be conducted independent of other military operations to support U.S. national security objectives. CMO can occur in friendly, neutral, or hostile operational areas to facilitate military operations and achieve U.S. objectives. CMO may include performance by military forces of activities and functions that are normally the responsibility of local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. CMO may be performed by designated civil affairs (CA), by other military forces, or by a combination of CA and other forces.<sup>55</sup>

## **3. Defense Support to Public Diplomacy**

DSPD consists of activities and measures taken by DoD components, not solely in the area of IO, to support and facilitate public diplomacy (PD) efforts of the USG. DoD contributes to PD, which includes those overt international information activities of the USG designed to promote U.S. foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers and by broadening the dialogue between American citizens and institutions and their counterparts abroad. When approved, MISO assets may be employed in support of DSPD as part of security cooperation initiatives or in support of U.S. embassy PD programs. Much of the operational level IO activity conducted in any theater will be directly linked to PD objectives. DSPD requires coordination with both the interagency and among DoD components.<sup>56</sup>

---

<sup>55</sup> Ibid., II-10.

<sup>56</sup> Ibid., II-10.

## **F. COMPARATIVE CHARACTERISTICS OF IO TERMS IN U.S. DOCTRINE: USAF FOCUS ON INFLUENCE OPS AND TECHNICAL CAPABILITIES**

After a brief look at the capabilities involved in IO as per the description of U.S. joint doctrine, it is beneficial to review differences and commonalities in definitions and characteristics of IO capabilities found within DoD, joint, and service-level doctrines. One of the notable differences can be observed in the U.S. Air Force's doctrinal approach toward IO, which refers to influence operations, electronic-warfare operations, and network-warfare operations. Influence operations is the employment of capabilities to affect behaviors, protect operations, communicate the commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander's objectives. They should influence adversary decision making, communicate the military perspective, manage perceptions, and promote behaviors conducive to friendly objectives. Counterpropaganda operations, psychological operations (PSYOPs), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, and public-affairs (PA) operations are the military capabilities of influence operations.<sup>57</sup> The term "computer-network operations" as used in joint publications is analogous to "network-warfare operations" (NW Ops) in Air Force doctrine. NW Ops are the integration of the military capabilities of network attack (NetA), network defense (NetD), and network warfare support (NS)<sup>58</sup>. Air Force doctrine also groups certain capabilities like IA under the realm of integrated-control enablers (ICE). ICEs are critical capabilities required to execute successful air, space, and information operations and produce integrated effects for the joint fight. These include intelligence, surveillance, and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and precision navigation and

---

<sup>57</sup> Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 11 January 2005, 9.

<sup>58</sup> *Ibid.*, 19.



timing (PNT). NetOps further encompasses IA, system and network management, and information dissemination management.<sup>59</sup> These commonalities and differences in IO capabilities are shown in Table 2.

<b>Term</b>	<b><i>Joint Doctrine Identification</i></b>	<b><i>Air Force Doctrine Identification</i></b>	<b><i>Army Doctrine Identification</i></b>	<b><i>Navy Doctrine Identification</i></b>
EW/EW Operations (EWO) (USAF-only term)	Core Capability	Capability	Core Capability	Core Capability
Electronic Attack	Action of EW	Military Capability of EWO	Component of EW	Subdivision of EW
Electronic Protect	Action of EW	Military Capability of EWO	Component of EW	Subdivision of EW
EW Support	Action of EW	Military Capability of EWO	Component of EW	Subdivision of EW
Computer Network Operations (CNO)/Network Warfare Ops (NW Ops) (USAF-only term)	Core Capability	Capability	Core Capability	N/A
Computer Network Attack (CNA)/Network Attack (NetA) (USAF-only term)	Action of CNO	Operational Activity of NW Ops	Core Capability	Core Capability
Computer Network Defense (CND)/Network Defense (NetD) (USAF-only term)	Action of CNO	Operational Activity of NW Ops	Core Capability	Core Capability
Computer Network Exploitation/Network Support (USAF-only term)	Related Enabling Operation of CNO	Operational Activity of NW Ops	Core Capability	N/A
Information Assurance	Supporting Capability	Integrated Control Enabler (part of Net Ops)	Supporting Capability	Supporting Capability
Influence Operations	N/A	Capability	N/A	N/A
PSYOPs	Core Capability	Military Capability of Influence Operations	Core Capability	Core Capability
Military Deception (MILDEC)	Core Capability	Military Capability of Influence Operations	Core Capability	Core Capability
Operations Security (OPSEC)	Core Capability	Military Capability of Influence	Core Capability	Core Capability

---

<sup>59</sup> Ibid., 39.

<b>Term</b>	<b><i>Joint Doctrine Identification</i></b>	<b><i>Air Force Doctrine Identification</i></b>	<b><i>Army Doctrine Identification</i></b>	<b><i>Navy Doctrine Identification</i></b>
		Operations		
Physical Attack/Physical Destruction	Supporting Capability	Supporting Capability of Influence Operations	Supporting Capability	Supporting Capability
Counterintelligence	Supporting Capability	Military Capability of Influence Operations	Supporting Capability	N/A
Public Affairs	Related Capability	Military Capability of Influence Operations	Related Activity	Supporting Capability
Counterpropaganda	Action taken by Public Affairs	Military Capability of Influence Operations	Supporting Capability	N/A
Counter-deception	N/A	N/A	Supporting Capability	N/A
*N/A = term not referred to in core doctrine document				
Sources: Joint Publication 3–13, <i>Information Operations</i> , 13 February 2006, II-1 through II-9; Air Force Doctrine Document (AFDD) 2–5, <i>Information Operations</i> , 11 January 2005, 5–25; Field Manual 3–13, <i>Information Operations: Doctrine, Tactics, Techniques, and Procedures</i> , 28 November 2003, 1–14, 2–7, 2–8; and Navy Warfare Publication 3–13, <i>Navy Information Operations</i> , 2003, 13 and 2–6.				

Table 2. Common Information-Operations Terms<sup>60</sup>

## G. THE U.S. NAVY’S MOVE TOWARD INFORMATION DOMINANCE

What all these potential adversaries—from terrorist cells to rogue nations to rising powers—have in common is that they have learned that it is unwise to confront the United States directly on conventional military terms. The United States cannot take its current dominance for granted and needs to invest in the programs, platforms, and personnel that will ensure that dominance’s persistence.

U.S. Secretary of Defense Robert Gates, January 2009

The U.S. Navy Chief of Naval Operations officially established the U.S. Fleet Cyber Command (FCC) and re-commissioned the U.S. 10th Fleet on January 29, 2010. FCC and the 10th Fleet were created as part of the CNO’s

<sup>60</sup> Timothy P. Franz, Matthew F. Durkin, Paul D. Williams, Richard A. Raines, Robert F. Mills, *Defining Information Operations Forces*, Air & Space Power Journal Summer 2007: 56.

vision to achieve the integration and innovation necessary for warfighting superiority across the full spectrum of military operations in the maritime, cyberspace and information domains. This initiative will help raise information to the forefront of the Navy's 21<sup>st</sup>-century arsenal<sup>61</sup>.

The vision of the U.S. Navy's information dominance is to pioneer, field, and employ game-changing capabilities to ensure information dominance over adversaries and decision superiority for commander, operational forces, and the nation. As a concept, information dominance is the ability to seize and control the information domain high ground when, where, and however required for decisive competitive advantage across the range of Navy missions. Information dominance means freedom of action to maneuver and act—conduct offensive and defensive actions, kinetically and non-kinetically—at the intersection of maritime, information, and cyberspace domains. At this intersection, the Navy exploits deep penetration, expanded maneuver space and information advantage to deliver warfighting options and effects.<sup>62</sup> As noted in May 2010 by Vice Admiral David J. Dorsett, deputy chief of naval operations for information dominance, to achieve information dominance, the Navy must radically realign warfighting capabilities. It must transition from a Navy that relies on individual units managing their own electromagnetic spectrum to fleets and battle forces collectively achieving command and control over the electromagnetic spectrum in an automated fashion. This will require re-engineering the Navy, its concepts, weapons, battle-management systems, and people.

#### **H. ESTABLISHMENT OF THE NAVY'S INFORMATION-DOMINANCE CORPS**

We must deliver new concepts and operational capabilities. We're about creating whole warfighting capability based on seamless

---

<sup>61</sup> CNO stands up Fleet Cyber Command, Anchor Watch, March 2010: 8

<sup>62</sup> The U.S. Navy Vision for Information Dominance, May 2010: 2–4 retrieved from <http://www.insaonline.org/assets/files/NavyInformationDominanceVisionMay2010.pdf> on October 22, 2012.

networks, integrated sensors and data and analysis delivered to the warfighter.

Adm. Gary Roughead, former U.S. Chief of Naval Operations,  
July 2009<sup>63</sup>

The former-CNO of the U.S. Navy directed that the Navy be the most prominent and dominant service in the areas of intelligence, cyber warfare, command and control, electronic warfare, battle management, and knowledge of the maritime environment.<sup>64</sup> To make possible this aspiration, it was necessary to continue breaking down barriers between fields, professions, and skills—and ultimately create a dramatically more competent and influential information-focused work force for the future. To achieve this objective, the ex-CNO took a bold step in creating the Information Dominance Corps (IDC). Focusing on unity of effort and the capacity to direct a cadre of officers, enlisted, and their civilian counterparts, the IDC integrates information professionals (IPs), information warfare (IW), naval intelligence, and oceanography, space-cadre officers, and cyber-warfare engineers with aviation aerographers mates (AGs), cryptologic technicians (CTs), intelligence specialists (ISs), and information technician (IT) enlisted personnel, and with civilians in the Navy Defense Civilian Intelligence Program<sup>65</sup>. Figure 6 shows the merger of various cadres in the IDC.

---

<sup>63</sup> Space and Naval Warfare Systems Command, “Making the Navy’s Information Dominance Vision a Reality” retrieved from [http://www.public.navy.mil/spawar/Press/Documents/Publications/1.18.12\\_AFCEA\\_Kit\\_II.pdf](http://www.public.navy.mil/spawar/Press/Documents/Publications/1.18.12_AFCEA_Kit_II.pdf) on October 23, 2012.

<sup>64</sup> The U.S. Navy Vision for Information Dominance, May 2010: 9 retrieved from <http://www.insaonline.org/assets/files/NavyInformationDominanceVisionMay2010.pdf> on October 22, 2012.

<sup>65</sup> Cynthia R. Duke, “*Bridging the Gap in the Realm of Information Dominance: a Concept of Operations for the Naval Postgraduate School Center for Cyber Warfare*” Naval Postgraduate School Thesis, September 2010: 3–4.







<b><u>Officer</u></b> 	Information Professional (IP)  182X 642X 742X	Information Warfare (IW)  181X 644X 744X  Cyber Warfare Engineer 184X 743X	Intelligence (INTEL)  183X 645X 745X	Meteorology/Oceanography (METOC)  180X 646X
<b><u>Enlisted</u></b> 	Information Systems Technician (IT) 	Cryptologic Technician (CT) (CTI, CTM, CTN, CTR, CTT) 	Intelligence Specialist (IS) 	Aerographer's Mate (AG) 
<b><u>Other</u></b>	IT Civilian	Space Cadre  5500x 6206x Subspecialists	Intelligence Civilian	

Figure 6. Communities merged to form the Information Dominance Corps (IDC)<sup>66</sup>

In creating the IDC, a corps of 45,000 persons, the “main battery” of the U.S. Navy has been harnessed. The Navy’s IDC professionals, in junior grades, are required to strengthen and deepen their professional skills in their communities and subspecialties while obtaining a broader understanding of cross-corps disciplines. Senior enlisted, officers, and civilians within the IDC will be required to retain depth in specialty and subspecialty areas while broadening their professional expertise across information disciplines.<sup>67</sup>

<sup>66</sup>IDC Self Synchronization website, Information Dominance Corps (IDC) retrieved from <http://www.idcsync.org/about/idc> on Oct 18, 2012.

<sup>67</sup> The U.S. Navy Vision for Information Dominance, May 2010: 10. Accessed October 22, 2012. <http://www.insaonline.org/assets/files/NavyInformationDominanceVisionMay2010.pdf>.

U.S. Naval leadership is looking to create a set of senior professionals who will become increasingly capable of managing and leading across the information domain. This will require some alterations to education, training, and career paths. The fundamentals will remain the same, but the Navy will be placing greater demands on IDC senior leaders. Indeed, expanding one's knowledge and skill is at the very foundation of what it means to become an information-dominance professional.<sup>68</sup>

## **I. THE U.S. ARMY'S MOVES TOWARD INFORM-AND-INFLUENCE ACTIVITIES**

Army forces conduct unified land operations in populated areas that require them to contend with the attitudes and perceptions of many audiences within and beyond their area of operations. *Field Manual 6-0, Mission Command* (June 2011) established the new mission-command warfighting function (MC WfF) and launched the Army's evolution of information operations to inform and influence activities (IIA). "Inform and influence" activities focus on all audiences within the information environment, which include domestic and foreign friendly, neutral, adversarial, and enemy. It is also in line with the new definition for IO and emerging joint doctrine, as it enables commanders with multiple information-related capabilities to evaluate and use available internal, or request external, resources to inform or influence selected populaces, actors, or audiences to support mission objectives. They do this through inform and influence activities—the integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform U.S. and global audiences; influence foreign audiences; and affect adversary and enemy decision making.<sup>69</sup> The two distinct lines of efforts, i.e., inform and influence, are described in Figure 7.

---

<sup>68</sup> Ibid.

<sup>69</sup> Information Operations Primer, U.S. Army War College, November 2011: 69.

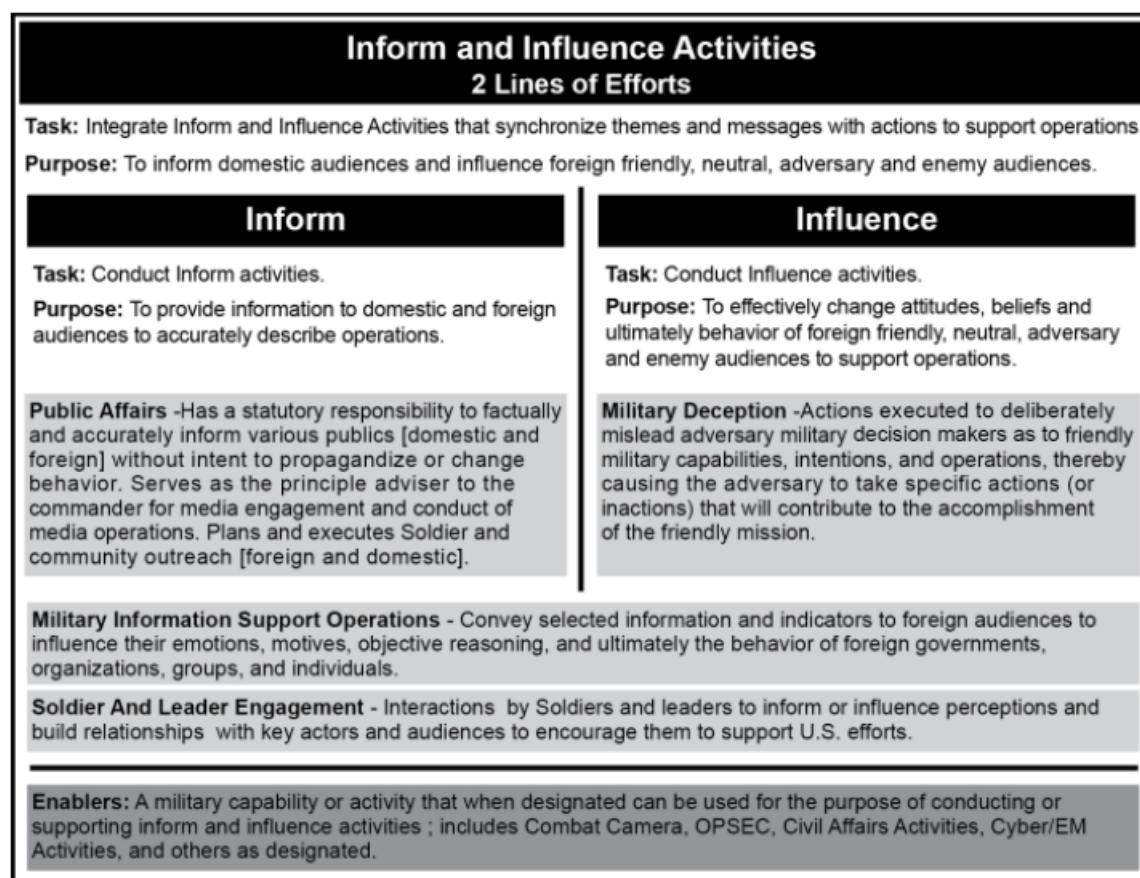


Figure 7. Army Inform-and-Influence Activities<sup>70</sup>

Information-related capabilities within inform and influence activities include, but are not limited to, the following areas (also depicted in Figure 8).<sup>71</sup>

- Public affairs
- Military information support operations
- Soldier and leader engagement
- Combat camera
- Military deception
- Cyber electromagnetic activities (electronic warfare, computer network operations, network operations, information security)
- Operations security

<sup>70</sup> Ibid., 9.

<sup>71</sup> Ibid., 70.

- Civil-affairs operations
- Special technical operations
- Commander-designated enablers (other)

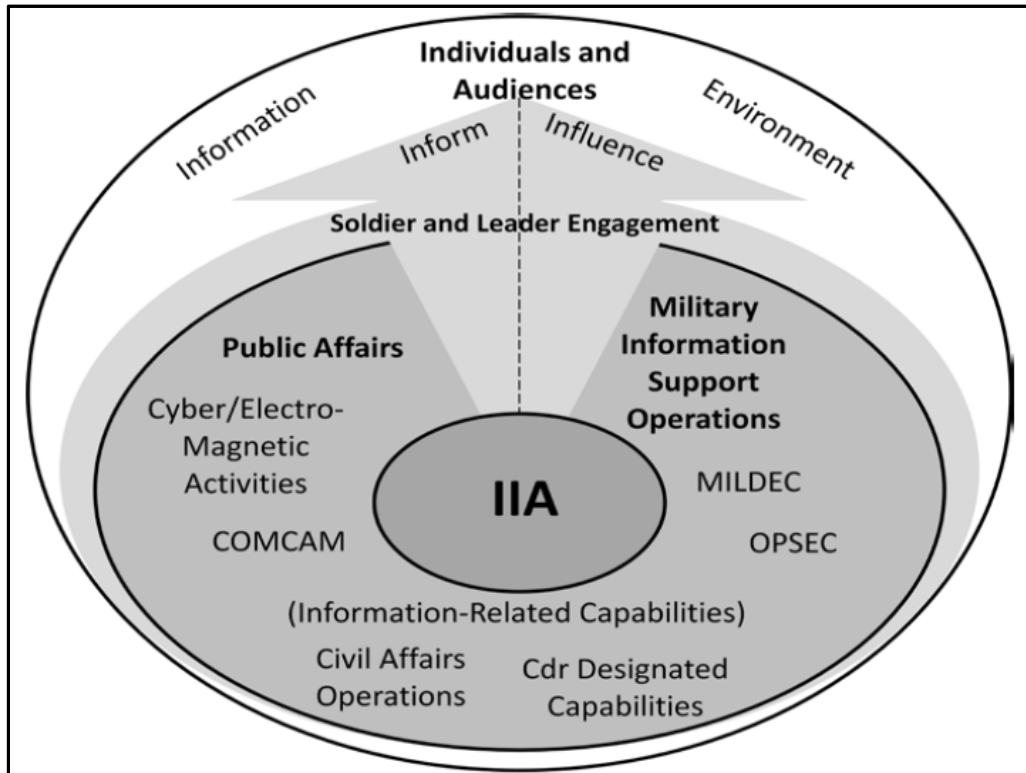


Figure 8. Integration of Information-Related Capabilities to affect the Information Environment

Recognizing the importance of operations in cyberspace, draft Army doctrine labels CNO and EW capabilities as falling within the newly defined area of “cyber/electromagnetic activities.” This construct is presented in Figure 9, below.



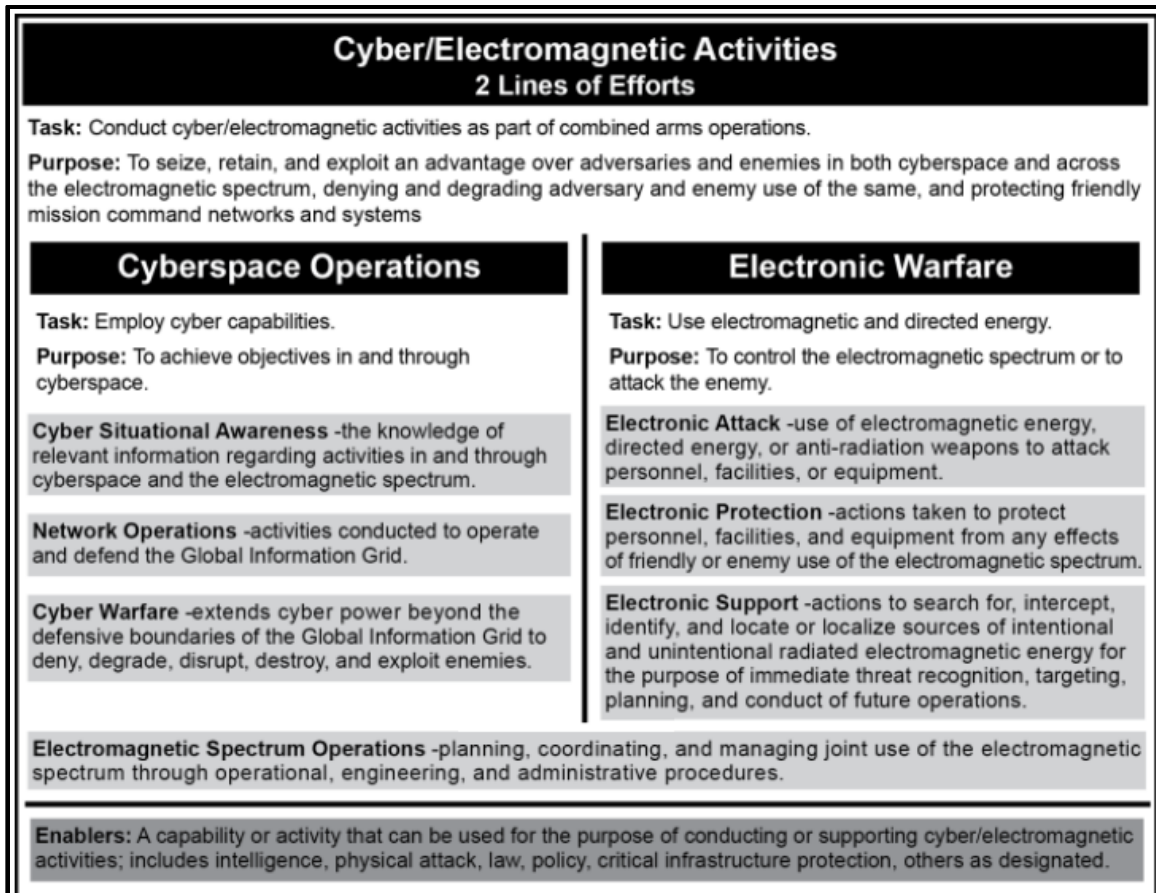


Figure 9. Army Cyber/Electromagnetic Activities

Cyber-electromagnetic activities seize, retain, and exploit advantages in cyberspace and the electromagnetic spectrum, enabling Army forces to retain freedom of action while denying freedom of action to enemies and adversaries. Cyber-electromagnetic activities are divided into two lines of effort: cyberspace operations and electronic warfare, as described in Figure 4, above. Within these two lines of effort are six subcomponents: cyber-network operations, cyber warfare, electronic attack, electronic protection, electronic-warfare support, and electromagnetic-spectrum operations.<sup>72</sup>

<sup>72</sup> Ibid., 74.

## **J. THE U.S. MARINE CORPS (USMC'S) APPROACH TO IO**

In general, the U.S. Marine Corps is tasked to provide Marine forces for service with combatant commanders. It is essential that these forces be manned, trained, and equipped with the means to directly or indirectly affect the behavior of hostile actors, friendly and neutral parties/organizations, and potential or realized adversaries throughout the full spectrum of conflict. To achieve this, Marine forces component commands and subordinate Marine air-ground task forces (MAGTFs) must be capable of conducting integrated IO; be postured to support and conduct actions necessary to influence adversary information, information-system operations, and decision making; and be able to assure, protect, and defend similar Marine forces' capabilities. Without IO capable Marine forces, the commander's requirement to secure, shape, and ultimately condition the operational environment can never be fully met.<sup>73</sup>

The U.S. Marine Corps Information Operations Program (MCIOP) was introduced in June 2008 to provide guidance and a future roadmap on the subject of IO.<sup>74</sup> It refers to U.S. JP 3–13 as the doctrinal foundation for Marine Corps IO, along with U.S. DoD directives on the subject. Per the promulgation order, the MCIOP seeks to integrate information operations down to the lowest levels of the Marine Corps in order to deny or degrade the ability of hostile and non-hostile actors to disseminate their message and, if desired, to modify it to USMC benefit while simultaneously preventing those same hostile messages from negatively affecting USMC decision-making processes. Integration of IO is an essential part of USMC routine operations in the expeditionary and joint environments. Properly executed, it can help prevent a crisis or conflict; failing prevention, IO can both mitigate adversaries' actions and enhance our own.<sup>75</sup>

---

<sup>73</sup> Marine Corps Order 3120.10, Marine Corps Information Operations Program (MCIOP), 30 June 2008: 2.

<sup>74</sup> Ibid.

<sup>75</sup> Ibid.

The USMC established the Marine Corps Information Operations Command (MCIOC) in 2008.<sup>76</sup> The primary mission of the MCIOC is “to provide MAGTF commanders and the Marine Corps a responsive and effective full-spectrum IO planning and PSYOPs delivery capability by means of deployable support teams and a comprehensive general support IO reach-back capability in order to support the interaction of IO into Marine Corps operations.”<sup>77</sup> Though IO capabilities recognized by USMC IO doctrine (MCWP 3–40.4, MAGTF Information Operations, 9 Jul 2003) is generally aligned with the joint publication, the MCIOC exerts more emphasis to train subject-matter experts (SME) in the areas of:

- 1) Mission planning
- 2) Threat and nodal analysis<sup>78</sup>
- 3) Electronic warfare
- 4) Military deception
- 5) Operations security
- 6) Psychological operations
- 7) Computer network operations
- 8) The supporting capability of combat camera
- 9) The related capability of civil military operations
- 10) Regional IO target expertise

## **K. SUMMARY**

The study of U.S. joint and services IO doctrines provides detailed and knowledgeable insight on the philosophy behind IO missions in each service and their adopted methodology to effectively employ this facet of warfare. It can be

---

<sup>76</sup> Marine Corps Bulletin 5400 of 14 March 2008 (CMC Washington DC CDI TFS 141153Z Mar 08, Establishment of MCIOC Phase One).

<sup>77</sup> Attachment I Interservice Support Agreement #M00264–09098–409. Accessed October 30, 2012. [www.quantico.usmc.mil/download.aspx?Path=/Uploads/Files/...](http://www.quantico.usmc.mil/download.aspx?Path=/Uploads/Files/...)

<sup>78</sup> The analysis of the adversary’s C2 system to determine critical and vulnerable nodes is called nodal analysis. Reference MCWP 3–40.4, “Marine Air-Ground Task Force Information Operations,” July 2003, 1–7.

seen from the study that, of late, each military service has distinctly approached IO focusing on certain peculiar expertise and capabilities that are most supportive to the missions, objectives, and existing competencies of that particular service. For instance, the U.S. Army now has a more matured approach toward MISO by evolving IO into inform and influence activities (IIA) in their doctrine. This is likely a result of their recent combat experiences in Iraq and Afghanistan, where the Army was simultaneously engaged in fighting an adversary in a foreign country while conducting collaboration, cooperation, and confidence building with a less hostile or neutral general local population. The U.S. Navy is moving toward information dominance, as defined above, in an effort to network together all sensors, irrespective of their operating domains, to present the commander or decision maker with a complete informational picture of the area of interest. This is part of a logical movement to shift from platform-centric to information-centric mode of warfare in order to economize assets, resources and manpower. The U.S. Air Force doctrine has relatively more emphasis on EW and networks (both computer and communications) management and protection. Certain organizations have been organized to look after these critical aspects of EW and network warfare operations. USAF doctrine also talks about ICE, a group of certain key capabilities vital in the gain-and-exploit tactics used in today's air battles. The U.S. Marine Corps' IO doctrine and MCIOP are generally aligned to joint publications without any evolutionary change in theory or procedure. However, MCIOP highlights certain fields of expertise that are relatively more involved in, and critical to, expeditionary warfare requirements encountered frequently by the Marines.

## **IV. U.S. JOINT AND SERVICE LEVEL IMPLEMENTATION OF INFORMATION OPERATIONS**

### **A. INTRODUCTION**

IO is not considered merely a force enabler anymore; rather it is an important instrument of national power comparable to air power and sea power. The U.S. DoD has given an eminent place to IO in all the major armed forces organizations, from combatant commands, their sub-unified commands, and service components, down to lower-tier military formations. A study of U.S. implementation of IO gives a fair amount of knowledge as how to constitute IO setup in a military organization and how to disperse human resource in order to accrue maximum benefits. Before taking a detailed look at IO-specific organizations and manpower management, it is beneficial to take a brief look over the general scheme under which U.S. armed forces are organized and governed.

The military organization of the U.S. DoD is composed of the Office of the Secretary Defense, Joint<sup>79</sup> Chiefs of Staff, Joint Staff, departments of the Army, Navy, and Air Force, and nine unified combatant commands. An overall organizational diagram of U.S. DoD depicting its major organs is shown in Figure 10 below. Since U.S. combatant commands are an important component for the execution of U.S. military policy, their brief function and organization is covered in Appendix A.

---

<sup>79</sup> The term 'joint' formally defined as, "involving two or more Services of the same nation," and the term 'combined' as, "applying to organizations, plans, and operations of two or more nations." This information is taken from U.S. Joint Staff Officers Guide-1997, chapter 2, *Joint Organization and Staff Functions*. Accessed November 13, 2012. [http://www.fas.org/man/dod-101/dod/docs/pub1\\_97/Chap2.html](http://www.fas.org/man/dod-101/dod/docs/pub1_97/Chap2.html)

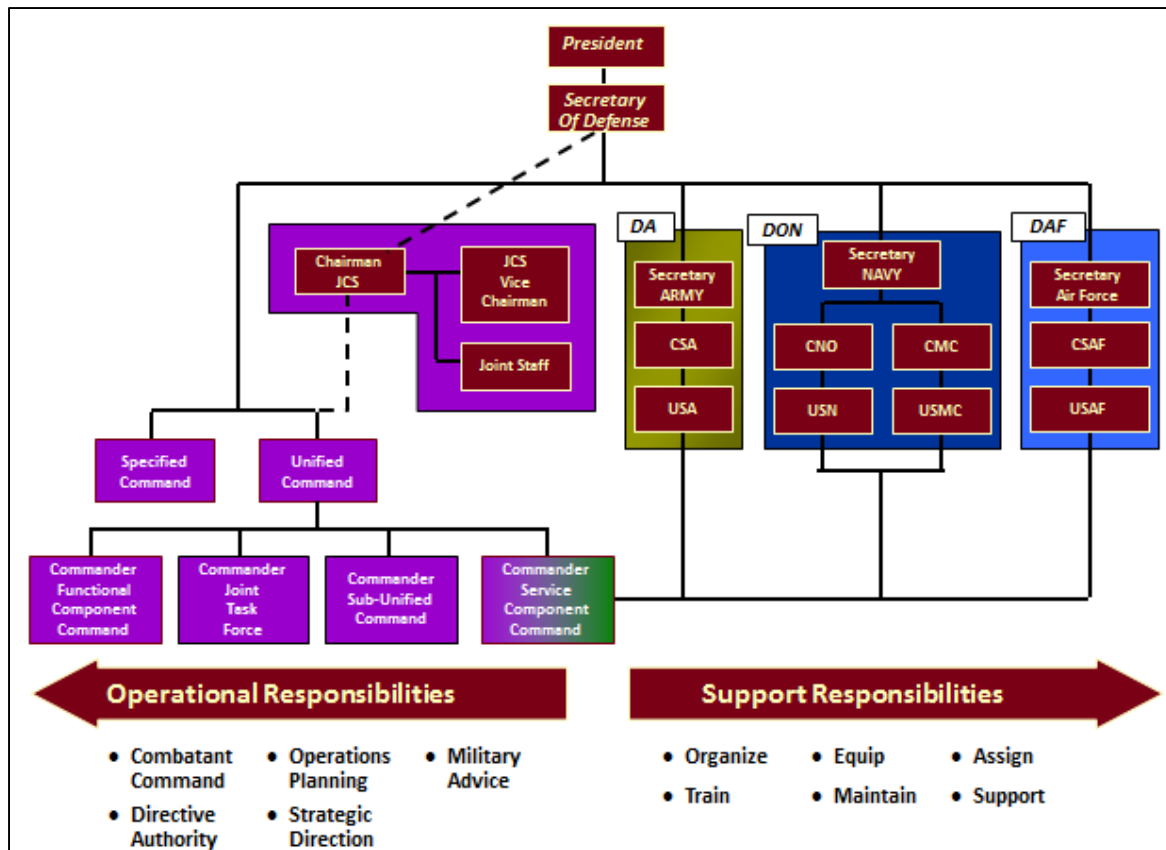


Figure 10. Military Organization of U.S. DoD<sup>80</sup>

## B. IO ORGANIZATION AT THE U.S. JOINT-STAFF LEVEL

### 1. General<sup>81</sup>

At the joint-staff level in the Pentagon, the deputy director for global operations (DDGO J-39) is responsible to the director for operations (DJ-3) and the Chairman of the Joint Chiefs Of Staff (CJCS) for providing expertise and advice in coordinating joint global operations, to include information operations (IO). Appropriate representatives from information-related capabilities as well as the special staff, service/functional components, and appropriate national

<sup>80</sup> This figure has been taken from a presentation prepared by Col Bob Hume on DoD Education 2009. Accessed October 31, 2012.  
<https://dde.carlisle.army.mil/documents/courses.../ppt/2208-UCP.ppt>

<sup>81</sup> Information in this section is taken by abridging details from U.S. Army War College IO Primer, November 2011, 127–137.

agencies serve as members of the J-39. The DDGO is responsible for IO activities, developing joint IO policy and doctrine, and coordinating with the Office of the Secretary of Defense (SecDef), combatant commands, services, defense agencies, other staff directorates, the intelligence community, and interagency on IO issues/actions. In addition, the DDGO is the focal point for all special technical operations (STO).

As of 1 October 2011, The Joint Information Operations Warfare Center (JIOWC) became a chairman-controlled activity (CCA) under the supervision of the DJ-3. This change has been discussed in detail in the next section. CCAs are specialized organizations designed to address unique areas that are of joint interest. The JIOWC supports the joint staff and combatant commands in DoD efforts to integrate joint information-related capabilities. The director, JIOWC, reports to the DJ-3 via the J-39.

## **2. Organization<sup>82</sup>**

The DDGO contains five IO-focused divisions as described in the following paragraphs:

### ***a. Computer Network Operations Division (CNOD)***

CNOD advises the SecDef and CJCS, through the DJ-3, on computer network operations. Additionally, CNOD provides analyses and recommendations for the integration and synchronization of global cyberspace operations, including defense, exploitation and attack; network operations (NETOps); and information assurance/cyber security. CNOD also supports COCOMS to meet combatant commander requirements and interfaces with the U.S. Government Interagency on operational employment and de-confliction of military CNO.

---

<sup>82</sup> Ibid.

***b. Information Operations Division (IOD)***

IOD facilitates and coordinates special capabilities and electronic warfare (EW) for the chairman, in support of all COCOMs, SecDef and select interagency partners. Additionally, IOD educates operators to better plan and employ military information operations. IOD consists of the following branches: combatant command support, plans support, electronic warfare, intelligence community liaisons, strategic multi-layer analysis management, IO policy and doctrine.

***c. Military Information Support Division (MISD)***

MISD provides expertise and advice on MISO employment to achieve national, strategic, and theater military objectives. It develops and provides guidance to, and coordinates with, COCOMs and services; reviews COCOM operation plan (OPLAN) requirements; develops concepts and prepares MISO plans; develops and coordinates joint MISO doctrine; publishes joint MISO doctrine; and publishes MISO supplements to the joint strategic capabilities plan and staff deployment orders. MISO consists of the following branches: geographic combatant command support and program and doctrine.

***d. Special Actions Division (SAD)***

SAD has primary responsibility for MILDEC and will work directly with JIOWC/Mission Support Division and with the Defense MILDEC Program Office as primary stakeholders to ensure community-wide equities are maintained and synchronized. SAD is composed of the support activities branch and the tactical-security branch.

***e. Joint Information Operations Warfare Center (JIOWC)***

Known as Joint Information Operations Center (JIOC) until 2006. The JIOWC assists the joint staff in improving DoD ability to meet COCOM information-related requirements, improves development of information related



capabilities, and ensures operational integration and coherence across COCOMs and other DoD activities. The main functions of the center are:

- Joint IO assessment
- Joint IO force development
- Joint operations security
- Joint military deception
- Coordinate and integrate DoD IO operational support for joint commanders

Some of the important capabilities provided by JIOWC are:

- Provides IO subject-matter experts with special emphasis on military deception and operations security
- Maintains a cadre of intelligence professionals tightly focused on the IO problem set
- Maintains a habitual working relationship with the IO staffs of the combatant commanders and service elements
- Provides focused and tailored IO planning products

### **C. REORGANIZATION OF IO IN THE U.S. DOD<sup>83</sup>**

In order to address questions relating to roles and missions, definitions, management, resources, training and education in the areas of strategic communication (SC) and IO, the U.S. Secretary of Defense ordered a SC and IO front-end assessment (FEA) in 2010. Based on this assessment, on October 1, 2010, the principal staff-advisor function and responsibility for IO oversight and management moved from the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Policy (USD[P]). The Secretary of Defense directed that the Chairman of the Joint Chiefs of Staff (CJCS), at the joint force level, will reorganize joint force IO development and management by assigning proponentcy for joint IO to the joint staff. Furthermore, responsibilities for individual capabilities of IO have been assigned to the following organizations:

---

<sup>83</sup> Information in this section is taken from U.S. Secretary of Defense Memorandum "Strategic Communication and Information Operations in the DoD" of January 25, 2011.

MISO is assigned to U.S. Special Operations Command, Cyber and EW are assigned to U.S. Strategic Command, and MILDEC and OPSEC are assigned to the joint staff.

As part of the same reorganizational process, the Chairman of the Joint Chiefs of Staff has reorganized elements of the Joint Information Operations Warfare Center (JIOWC), previously assigned to USSTRATCOM. The JIOWC's Joint Electronic Warfare Division remains assigned to USSTRATCOM and the remaining elements of the JIOWC were aligned with the Joint Staff. By bringing the JIOWC under the supervision of CJCS, it will continue to benefit the COCOMs and will remove some of the limitations placed upon it by its subordination to STRATCOM.

The following benefits are anticipated from the above mentioned reorganization /assignments:

1. Creating a single proponent for joint IO integration with designated, clear capability proponents.
2. Improving the U.S. DoD's ability to meet combatant command requirements and improving development of information-related capabilities.
3. Ensuring operational integration and coherence across combatant commands and the interagency.

Each COCOM has a designated staff (J-3 and its subordinate staff) in the command's headquarter to undertake IO-related duties. Moreover, service components and various task forces under COCOM also possess specified IO staff. Two of the functional combatant commands (USSTRATCOM and USSOCOM) have been entrusted with the responsibility of designated IO capabilities, as discussed above. Due to their increased role in the field of IO, these commands will be described briefly in ensuing paragraphs.

#### **D. U.S. STRATEGIC COMMAND (USSTRATCOM)**

##### **1. Mission**

USSTRATCOM's primary responsibility is the stewardship and employment of U.S. nuclear weapons and to detect, deter, and prevent attacks

against the United States and its allies and to join with the other combatant commands to defend the nation should deterrence fail.<sup>84</sup> This command combines the synergy of the U.S. legacy nuclear command and control mission with responsibility for space operations; global strike; DoD information operations; global missile defense; and global command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), and combating weapons of mass destruction. This dynamic command gives national leadership a unified resource for greater understanding of specific threats around the world and the means to respond to those threats rapidly.<sup>85</sup>

## **2. History**

USSTRATCOM was established October 1, 2002. The missions most directly associated with USSTRATCOM and its predecessors are deterrence and global strike. These were the missions of Strategic Air Command (SAC) from 1946 to 1992 and of the first USSTRATCOM from 1992 to 2002. On June 1, 1992, SAC was replaced by a new unified command, USSTRATCOM. The new command's primary mission was to deter attack, especially nuclear attack, on the United States and its allies and, if deterrence failed, employ nuclear forces in response.<sup>86</sup>

The U.S. military began operating in space in the late 1950s, with many of the early systems developed to meet SAC's needs for surveillance, warning, meteorology, and communications. By 1985, space activities had grown to such a scale that U.S. DoD created a new unified command, USSPACECOM, to manage military space operations. The U.S. DoD then took initiative to merge USSTRATCOM and USSPACECOM, which led to the creation of the current USSTRATCOM in 2002. The U.S. military's reliance on computer networks grew

---

<sup>84</sup> Feickert op. cit., 19.

<sup>85</sup> U.S. Strategic Command official website. Accessed October 28, 2012.  
<http://www.stratcom.mil/about/>

<sup>86</sup> Feickert op. cit., 19.

exponentially in the 1980s and 1990s. U.S. national leaders took steps to protect defense networks in 1998, creating a Joint Task Force for Computer Network Defense and assigning it to USSPACECOM. As computer attacks against DoD become more sophisticated and frequent, there were calls to place greater emphasis and visibility on cyber operations. Former U.S. Defense Secretary Robert Gates favored a new sub-unified command under USSTRATCOM that would recombine offensive and defensive computer-network operations. Established 21 May 2010, U.S. Cyber Command (USCYBERCOM) was fully operational on October 31, 2010.<sup>87</sup>

### **3. Command Subcomponents.**

As mentioned above, the USSTRATCOM consists of a sub-unified command, namely U.S. Cyber Command (USCYBERCOM), besides several joint functional and service components. As far as relevance to IO objectives is concerned, the role of USCYBERCOM is critical in conducting CNO and IA functions. USCYBERCOM centralizes the command of cyberspace operations, strengthens U.S. DoD cyberspace capabilities, and integrates and bolsters DoD cyber expertise. It consequently improves the U.S. DoD's capabilities to ensure resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace. USCYBERCOM's efforts also support the armed services' ability to confidently conduct high-tempo, effective operations and protect command-and-control systems and the cyberspace infrastructure supporting weapons-system platforms from disruptions, intrusions and attacks.<sup>88</sup> A synopsis of USSTRATCOM command subcomponents, including functional and service elements, is given in Appendix B.

---

<sup>87</sup> Ibid., 20.

<sup>88</sup> This information is retrieved from U.S. Cyber Command Fact Sheet published by U.S. DoD Office of the Public Affairs. Accessed November 17, 2012.  
[http://www.defense.gov/home/features/2010/0410\\_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf](http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf)

## **E. U.S. SPECIAL OPERATIONS COMMAND (USSOCOM)**

### **1. Mission**

USSOCOM's primary mission is to organize, train, and equip special-operations forces (SOF) and provide those forces to the geographic combatant commanders under whose operational control they serve. USSOCOM also develops special-operations strategy, doctrine, and procedures for the use of SOF and also develops and procures specialized, SOF-unique equipment for its assigned forces. USSOCOM is also the lead COCOM for synchronizing DoD planning against terrorists and their networks on a global basis. USSOCOM can execute global operations against terrorist networks when directed to do so by the president or secretary of defense.<sup>89</sup>

### **2. History**

The 1980 Desert One tragedy<sup>90</sup> and the 1983 loss of 237 U.S. Marines in Beirut, combined with the command-and-control problems experienced during Grenada in 1983, heightened apprehensions about the DoD's ability to manage the services, including special-operations forces who were "owned" by their respective services. The U.S. president approved the establishment of USSOCOM on April 13, 1987, and the DoD activated this new unified command on April 16, 1987.<sup>91</sup>

---

<sup>89</sup> Feickert op. cit., 15.

<sup>90</sup> The disastrous "Desert One" Rescue Operation began in the evening of April 24, 1980, when U.S. military forces launched a bold but failed attempt to rescue their fellow American citizens and their nation's honor from captivity in Tehran. In the early hours of April 25, the effort ended in fiery disaster with a loss of eight U.S. soldiers at a remote spot in Iran known ever after as Desert One. This information is taken from Otto Kreisher article in the Air Force Magazine posted on October 13, 2001. Accessed November 4, 2012. <http://www.freerepublic.com/focus/f-news/547308/posts>

<sup>91</sup> Feickert op. cit., 15–16.

### **3. IO Core and Related Capabilities within USSOCOM Purview<sup>92</sup>.**

#### ***a. Military Information Support Operations (MISO)***

A vital part of the broad range of U.S. political, military, economic, and information activities used by the U.S. government to secure national objectives, MISO disseminates truthful information to foreign audiences in support of U.S. policy and national objectives. Used during peacetime, contingency operations, and declared war, these activities are not a form of force, but are force multipliers that use nonviolent means in often-violent environments. Persuading rather than compelling physically, they rely on logic, fear, desire or other mental factors to promote specific emotions, attitudes, or behaviors. The ultimate objective of U.S. military information support operations is to convince target audiences to take action favorable toward the United States and its allies. The importance and effectiveness of military information support operations has been underscored during Operations Enduring Freedom and Iraqi Freedom.

#### ***b. Civil Affairs (CA)***

CA units support military commanders by working to minimize the effect of civilians in the battle space and by coordinating with civil authorities and civilian populations in the commander's area of operations to lessen the impact of military operations on them during peace, contingency operations, and declared war. Civil affairs forces support activities of both conventional and SOF, and are capable of assisting and supporting the civil administration in their area of operations. Long after the guns have fallen silent, the men and women of civil affairs continue to provide assistance to foreign governments and stabilize regions in turmoil.

---

<sup>92</sup> Information in this section is taken from U.S. Army War College IO Primer, November 2011, 146.

### **c. Components**

USSOCOM has four component commands from each service (Army, Navy, Air Force and Marine Corps) and one sub-unified command. With the IO perspective in view, the Army component known as U.S. Army Special Operations Command (USASOC) contributes directly in provision of psychological operations and civil affairs forces to USSOCOM for deployment as required to other unified combatant commands and country ambassadors around the world. They also provide logistics and signal support to these operations.<sup>93</sup> A general description of all USSOCOM components is attached as Appendix C.

## **F. IO ORGANIZATION IN THE U.S. ARMED SERVICES**

IO organization in U.S. joint staff and realignment of various IO capabilities has been described earlier in the chapter. IO organization at the services level is also evolving continuously and undergoing significant changes from time to time. These organizations will be briefly covered here.

### **1. The U.S. Army**

At the top tier in American hierarchy under the Chief of Staff U.S. Army (CSA), designations of G3/G5/G7 represent deputy chiefs of staff for operations. At the corps/division level, G3 is associated with operations and plans, G5 with civil affairs, and G7 with information operations.

The USA's information operations are now evolved into inform and influence activities (IIA) and cyber/electromagnetic activities as new mission command warfighting functions (WFF) as discussed in Chapter III. Accordingly, the final draft of U.S. Army Doctrine FM 3-13 on IIA now designates G7 (S-7 for brigade level and lower) as responsible for integration of information-related capabilities. Per the doctrine,

---

<sup>93</sup> This information is taken from USASOC web page of Global Security.org. Accessed on November 18, 2012. <http://www.globalsecurity.org/military/agency/army/arsoc.htm>.

The G-7 (S-7), inform and influence activities officer, serves as the commander's primary coordinating staff officer for integrating information-related capabilities and assessing measures of performance (MOP) and measures of effectiveness (MOE) in accordance with the plan. To best advise the commander, the G-7 (S-7) must understand the information and operational environments.<sup>94</sup>

The G-7 will not have the responsibility for synchronizing all cyber/EW activities but will conduct coordination to ensure these activities support IIA activities.<sup>95</sup>

## **2. The U.S. Navy**

The top-level positions of deputy chief of naval operations (DCNO) for intelligence (N2) and DCNO for communications (N6) in the Office of the Chief of Naval Operations (OPNAV) were merged on October 1, 2009. The new directorate is headed by a three-star flag officer known as the DCNO for information dominance (OPNAV N2/N6). In this plan, manpower and readiness resources for the Information Dominance Corps have been consolidated under N2/N6 to enable informed program wholeness and warfighting capability trades for information, cyber, and electronic warfare systems. Additionally, personnel, training and readiness personnel from N1 (manpower and personnel) and N4 (fleet readiness and logistics) will be transferred to N2/N6 to enable more informed system centric trades and warfighting integration. N2/N6 is responsible for Integration and Interoperability assessments for all warfare systems.<sup>96</sup>

According to ex-CNO of the USN Admiral Roughead remarks,

...this merger is in support of the establishment of Fleet Cyber Command, whose mission will be to serve as the central operational authority for networks, intelligence, cryptology/signals

---

<sup>94</sup> USA FM 3-13, "*Inform and Influence Activities- Final Draft*," Headquarters Department of the Army, Washington, DC, 25 October 2011: 4-1.

<sup>95</sup> U.S. Army War College IO Primer, November 2011: 9.

<sup>96</sup> Online article on U.S. Navy website, "CNO realigns OPNAV Staff." Accessed November 6, 2012. [http://www.navy.mil/submit/display.asp?story\\_id=65845](http://www.navy.mil/submit/display.asp?story_id=65845)



intelligence, information operations, cyber, electronic warfare and space in support of forces afloat and ashore. While N2/N6 will focus on investments to ensure future dominance, Fleet Cyber Command will focus on operations.<sup>97</sup>

### **3. The U.S. Air Force**

At the U.S. air-staff level, A2 is responsible for intelligence, surveillance and reconnaissance and A3/5 for operations, plans and requirements.<sup>98</sup> The Air Combat Command (ACC) and Air Force Space Command (AFSPC) are among the thirteen major/component commands of the USAF.<sup>99</sup> Both these major commands operate IO units to accomplish their assigned duties and assist joint forces.

The U.S. Air Force activated its cyber-focused, numbered air force, the 24th Air Force, under AFSPC back in 2009. This step was a major milestone in the combination of space and cyberspace operations within one command. The 24 AF provides combat-ready forces trained and equipped to conduct sustained cyber operations, fully integrated within air and space operations. It also enables combatant commanders with critical cyber component capabilities, ensuring a key element of joint and combined operations toward its global mission. The 24 AF has three major three wings in its organization: the 688th Information Operations Wing (IOW), the 67th Network Warfare Wing, and the 689th Combat Communications Wing.<sup>100</sup> The 688th Information Operations Wing delivers proven information operations and engineering infrastructure capabilities integrated across air, space and cyberspace domains. The 688th team comprises more than 1200 military and civilian members skilled in the areas of

---

<sup>97</sup> Online article on N2/N6 Reorganization. Accessed November 6, 2012.  
<http://www.dawnbreaker.com/portals/p3p/opnav/opnav-n2-n6.php>

<sup>98</sup> Information taken from official USAF website. Accessed November 7, 2012.  
<http://www.af.mil/information/afchain/index.asp>

<sup>99</sup> Information taken from official USAF website. Accessed November 7, 2012.  
<http://www.af.mil/publicwebsites/index.asp>

<sup>100</sup> Information taken from official USAF website. Accessed November 7, 2012.  
<http://www.afspc.af.mil/news/story.asp?id=123163863>

engineering installation, weaponeering, operations research, intelligence, communications and computer applications. The wing is further composed of two groups: the 318th Information Operations Group (IOG) and the 38th Cyberspace Engineering Group (CEG).<sup>101</sup>

#### **4. The U.S. Marine Corps<sup>102</sup>**

At the USMC staff level, the G-3/S-3 is responsible for IO. The future operations (FuOps) section, in conjunction with the Marine Air-Ground Task Force (MAGTF) fires and effects cell is responsible for overseeing the planning and coordination of the IO effort. MAGTF is the basic framework for deployable Marine units and carries a flexible structure that can vary in size per the requirements of the mission. The MAGTF IO officer, within G-3/S-3 FuOps, is mainly responsible for:

- The broad integration and synchronization of IO efforts.
- Responding directly to the G-3/S-3 for MAGTF IO.
- Participating, as a member, in the operational planning team (OPT) during all phases of planning to ensure coordinated operations.
- Preparing the IO appendix to the operation order (OPORD).
- Directing the efforts of core IO cell personnel as well as liaisons from external agencies.
- Coordinating and supporting IO activities of subordinate commands.

Established within a MAGTF and/or higher headquarters, the IO cell is a task-organized group that integrates information-related capabilities. A fully functioning IO cell plans for, monitors the execution of, and assesses the effects of IO across all MAGTF operations. The cell accomplishes this through extensive planning and coordination among all elements of the staff. The size, structure, and placement of the IO cell within the staff are tailored to meet the mission and

---

<sup>101</sup> Information taken from official USAF website. Accessed November 7, 2012.  
<http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15333>

<sup>102</sup> U.S. Army War College IO Primer, November 2011: 80–81.

commander's intent. Integration of intelligence into the information operations cell is critical to the planning, execution, and assessment of IO. In order to effectively engage the intelligence system, the IO staff clearly articulates intelligence requirements in order to facilitate G-2/S-2 staff to effectively work toward successful IO planning and execution.

## **G. SUMMARY**

Information operations are part of all major joint, service level, functional and geographical military organizations of the United States. The details covered in this chapter show only a glimpse of the enormous information-related activities conducted in the U.S. DoD and its constituent organizations. In order to remain abreast with latest trends of warfare and innovating technologies, IO forces and their structures have been changing continuously, particularly in the last decade or so. The expansion in these organizations and the development of new operational units also testify that the sphere of IO activities is consistently on the rise, both in areas where conflict or war exist and where peace is prevalent. It is also evident from the study that IO organization and its synchronization and coordination with other activities has received significant focus and emphasis from top leadership, because only a viable organizational plan and effective training methodology can ensure successful implementation within military activities.

THIS PAGE INTENTIONALLY LEFT BLANK

## **V. ESTABLISHING A VIABLE INFORMATION WARFARE CAPABILITY IN SMALLER MILITARIES**

### **A. INTRODUCTION**

Preparation for information warfare and the conducting of all phases of information operations at a national level requires an overarching policy, an implementing strategy developed by responsible organizations, and the operational doctrine and personnel to carry out the policy.<sup>103</sup> In the preceding chapter, the general contours of an IO organization in a well-established military structure, such as the U.S. armed forces, were presented. In smaller militaries, the structure of IO organization is usually much more limited in scope, either due to less IO-intensive strategic objectives, or financial constraints resulting from national economic conditions, or both. Identifying relevant and effective capabilities of IO that best suit the accomplishment of national-security interests is the primary requirement toward a comprehensive and all-encompassing IO policy of any nation. As a first step toward this goal, there should be a clear procedural understanding of policy and strategic level IW issues by the decision-making hierarchy of a country, to support the production of intellectual documentation.

### **B. INFORMATION WARFARE POLICY AND STRATEGY<sup>104</sup>**

#### **1. General**

The various capabilities that are grouped under the realm of information warfare are the means at the bottom of a classical hierarchy that leads from the ends (objectives) of national-security policy. The hierarchy proceeds from the policy to an implementing strategy, then to operational doctrine (procedures) and

---

<sup>103</sup> Edward Waltz, *Information Warfare Principles and Operations* (Norwood: Artech House, 1998), 139.

<sup>104</sup> Information in this section is taken by abridging and modifying details from Waltz, *Information Warfare*, 140–144.

a structure (organization) that applies at the final tactical level or the technical operations of IW. The hierarchy flows down from the security policy, with each successive layer in the hierarchy implementing the security objectives of the policy.

Table 3 illustrates this hierarchy with examples of typical representative documents that occur at each layer that help to achieve the ultimate goal of national security through IW. Although the table lists only military strategic, operational, and tactical documents, a comprehensive policy implementation must incorporate levels in all areas of the national infrastructure.

<b>Level (Authority)</b>	<b>Role Description</b>	<b>Typical Representative Documents</b>
Policy (government policymakers, defense ministry/department of defense)	Define the objects of security (interests), the security objectives for those interests, and their intent and willingness to apply resources to protect those interests.	National security policy, National Security Act, National cryptologic policy, National information warfare policy, etc.
Strategy (military joint staff, individual services)	Develop a plan to apply political, economic, psychological, and military force as necessary during peace and war to afford the maximum support to policies.	National security strategy, national military strategy, joint information warfare strategy, etc.
Operations (commander)	Establish organizations; plan resources; develop and test capabilities (e.g., human competencies legal, technical means); create concept of operations (CONOPS) to implement the strategy. Oversee development of doctrine.	Service doctrines for operations security, military deception, psychological operations, ew etc. Services' concept for information operations.
Tactics (warfighter)	Equip, train for, and deploy the technical means and tactical doctrine for application of those means to conduct IO.	Fleet/ field tactical manuals for specific IW capabilities, Training manuals, Standing instructions from operational commanders, etc.

Table 3. General Hierarchy of Policy, Strategy, and Operations to Address IW's Military Perspective

## **2. Security Policy**

Policy is the authoritative articulation of the position of an organization, defining its interests (the objects being secured), the security objectives for those interests, and its intent and willingness to apply resources to protect those interests. The interests to be secured and the means of security are defined by the policy. The policy may be publicly declared or privately held, and the written format must be concise and clear to permit the implementing strategy to be traceable to the policy.<sup>105</sup>

A security policy to harness the true potential of IW must assess the new vulnerabilities of a nation. Information threats go far beyond the traditional considerations of geographical limits and political settings. Therefore, the old security apparatus that safeguarded geographic and political positions must be assessed and renewed.

Identification of a national information infrastructure (NII) must be clearly made in the information-security policy. This infrastructure is very diverse in nature and contains military, other government agencies, and private stakeholders. The information, processes and structures are all vulnerable, thus their pertaining security responsibilities must be clearly defined in the policy to identify the object being protected.

The desired levels of information security that comes under information assurance (IA) must be well defined in the policy in terms of integrity, authenticity, confidentiality, nonrepudiation, and availability. Moreover, a nation must define its intent to use IO and its willingness to apply those weapons. This factor becomes highly important when deciding about what actions against the nation will constitute sufficient justification to launch information strikes and what levels of direct and collateral damage resulting from information strikes are permissible.

---

<sup>105</sup> Waltz, *Information Warfare*, 140.



A general representation of various functional tiers involved in the formulation of policy documents down to operations level tasks is illustrated in Figure 11. It can also be noted in the diagram that certain technical operations are related to each other and detailed coordination is required for their proper execution. Moreover, operations at the lowest tier of the tactical level contribute ultimately to the implementation of the stated policy.

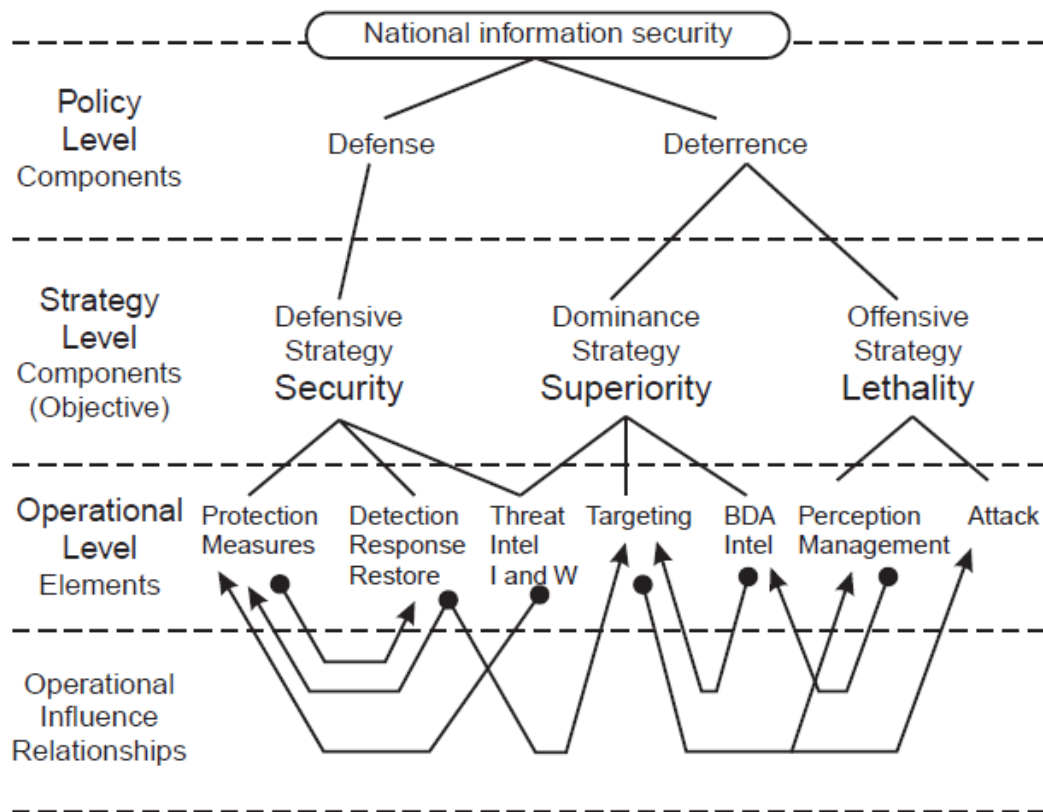


Figure 11. Fundamental hierarchy and components of a national information-security strategy<sup>106</sup>

<sup>106</sup> Waltz op. cit.: 145.

### 3. Security Strategy

National strategy<sup>107</sup> is the art and science of developing and using the political, economic, and informational powers of a nation, together with its armed forces, during peace and war, to secure national objectives. The national military strategy, normally approved by the Chairman of the Joint Chiefs of Staff in most countries, extends this to apply the armed forces to afford the maximum support to policies in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat. Strategists, in both military and business alike, debate the precise content, development, and implementation of strategy, but all recognize it must be a dynamic process, ever changing to adapt to the external environment to meet even a static policy position.<sup>108</sup>

Strategy is articulated in a plan, defining the means to implement policy. The strategic process (Figure 12) includes both strategy developing activities and a complementary assessment process that continuously monitors the effectiveness of the strategy.

---

<sup>107</sup> Strategy, per *JP 1-02*, is a prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives.

<sup>108</sup> Waltz, *Information Warfare*, 144.

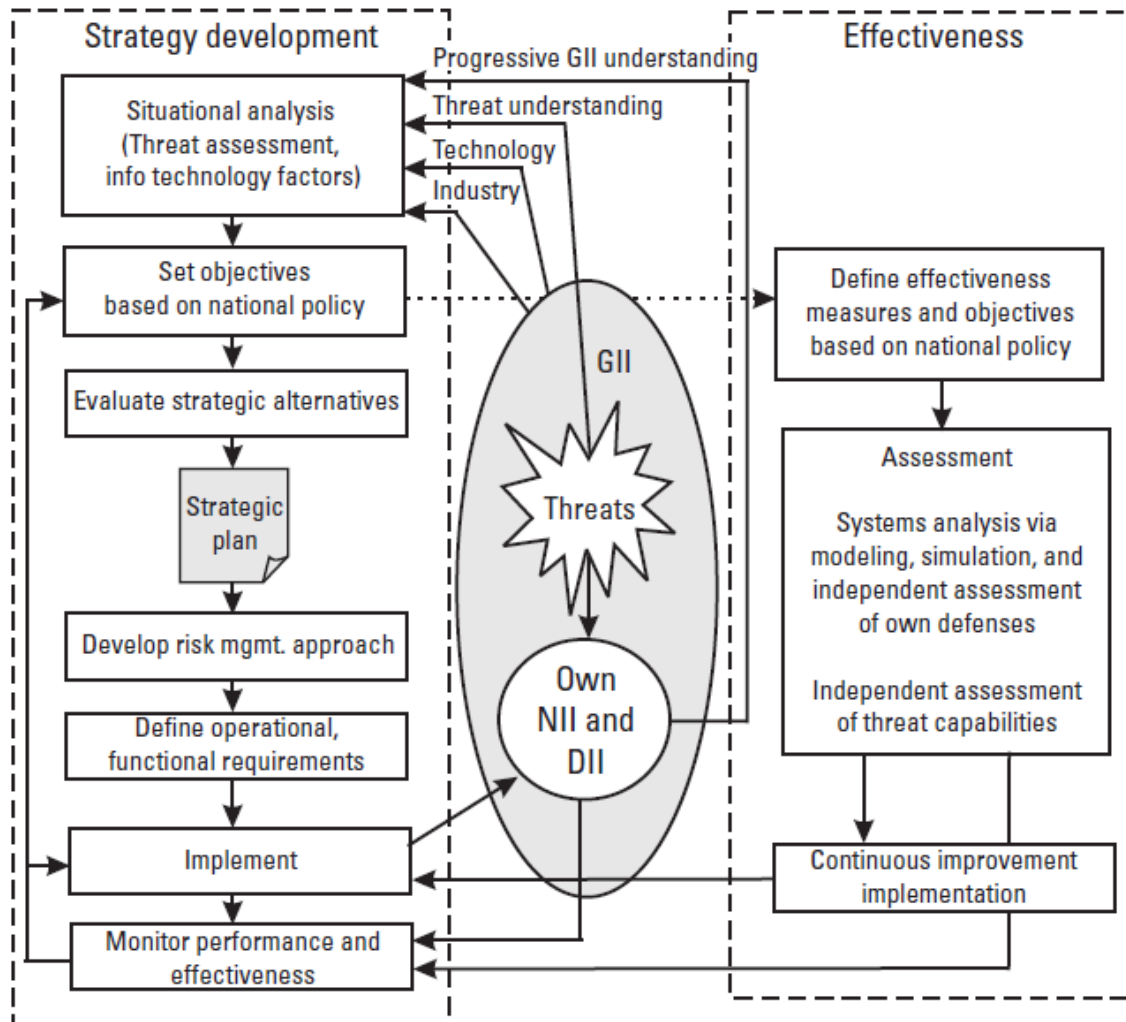


Figure 12. The strategic process includes strategy development and assessment elements.<sup>109</sup>

It is evident from the above figure that threats drive the formulation of objectives in strategy development. An accurate and correct assessment of all threats to the national information infrastructure is vital in this regard. The strategic objectives so formed are always in concordance with the national security policy. After development of the strategic plan, possible risks in strategy implementations are weighed and their consequences are considered.

<sup>109</sup> Waltz, *Information Warfare*, 146.

Consequently, operational requirements for organizations' structures, their associated research and development (R&D), and test and evaluation (T&E) requirements are determined for an overall budget allocation. Due consideration should be given to development of operational concepts, doctrines, and training. Throughout this process, effective monitoring of the performance of all activities ensures timely completion and implementation of the plan.

### **C. FEASIBLE IW ADAPTATION FOR SMALLER MILITARIES**

There are a small number of fundamental war principles that we cannot ignore without risk, and where, on the contrary, the application has always been successful.

Henri, Baron de Jomini (Précis de l'art de la guerre 1838;  
Summary of the Art of War, 1868).<sup>110</sup>

As was discussed in an earlier chapter, EW and CNO are comparatively new core capabilities added to IO's arsenal, whereas the rest of the core capabilities have been used in warfare since early ages. Similarly, when looking at the rest of the supporting and related capabilities, only IA and COMCAM are the products of recent technological advancements. The rest of the capabilities are based on older recognized warfighting principles. By their very nature, the capabilities of EW, CNO, and IA (when seen in the context of cyber related measures and activities) are technologically dependent and resource intensive. In smaller militaries, these capabilities can be difficult to introduce at their full capacity or to manage at maximum efficacy. However, a careful selection and implementation of various older and relatively inexpensive capabilities, from policies to strategic planning and operations, can prove to be extremely helpful in eradicating the common menaces of insurgencies and terrorism in an irregular and asymmetric environment. In the past, many IW theorists and practitioners have advocated attacking perceptual and physical levels of an information environment as complementary to conventional military warfare. Arguing for this stance, Major Yulin Whitehead, USAF, noted following in his paper,

---

<sup>110</sup> Daniel Ventre, *Information Warfare*, (London: ISTE Ltd, 2009), 114.

It is clear that while information may be used as a weapon, strategists must use it with caution and common sense. It is not a silver-bullet weapon. Rather, the strategist should plan the use of the information weapon in conjunction with more traditional weapons and employ it as a precursor weapon to blind the enemy prior to conventional attacks and operations.<sup>111</sup>

Before proceeding to the discussion of feasible IW capabilities in the perspective of developing countries, it is important to take a look at the predominant threat faced by militaries in these countries.

### **1. Insurgencies and Terrorist Activities in Developing Countries.**

From the study of insurgencies in the post-19th-century era, it is apparent that all insurgencies and uprisings have erupted in developing countries or regions in more prosperous nations that suffer from less development. Major instances include the Philippines (1902–1913), Malayan insurgency (1948–1989), Algerian War of Independence (1954–1962), Angola (1961–2002), Eritrean War of Independence (1961–1991), Vietnam (1955–1975), Iraq (2003–2008), Sri Lanka (1983–2009), and Afghanistan (2003–present).<sup>112</sup>

According to Global Terrorism Database (GTD)<sup>113</sup> empirical data from 1971 until 2007, developing countries are by far the most severely affected by terrorist attacks. Figure 13 below represents these data graphically and lists the

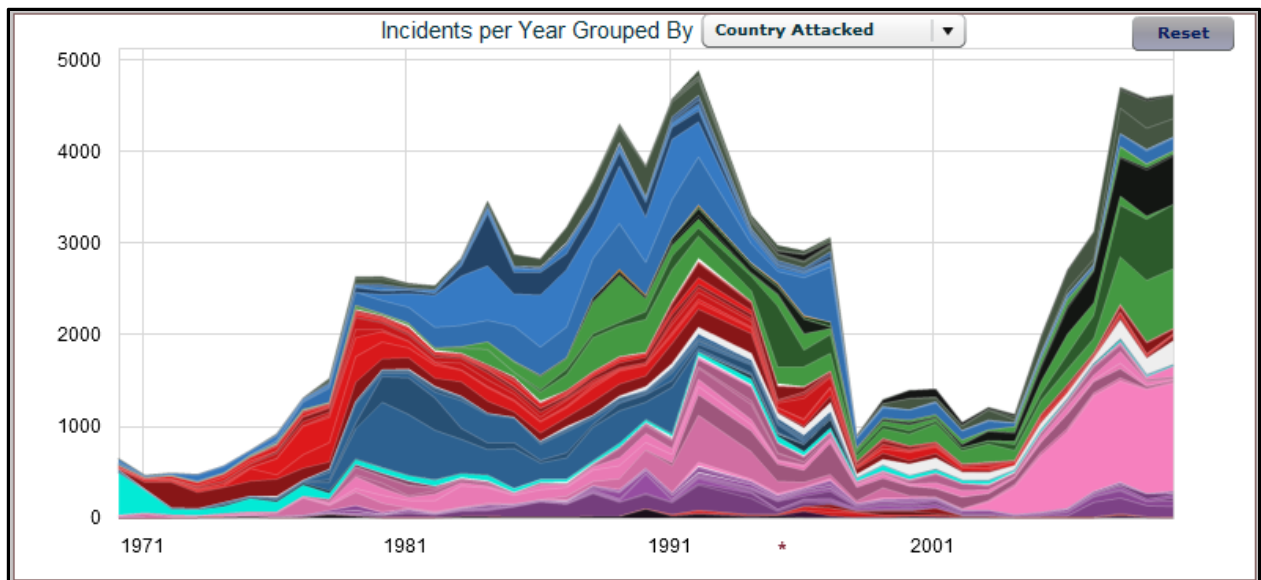
---

<sup>111</sup> Yulin Whitehead, *Information as a Weapon: Reality versus Promises*, Airpower Journal Fall 1997:50. Accessed November 15, 2012. [ics-www.leeds.ac.uk/papers/pmt/exhibits/548/whitehead.pdf](http://ics-www.leeds.ac.uk/papers/pmt/exhibits/548/whitehead.pdf)

<sup>112</sup> Rodney Graves, *A short course in the history of insurgency and counter-insurgency*, online resource. Accessed November 15, 2012. <http://wizbangblog.com/content/2011/06/01/a-very-short-course-in-the-history-of-insurgency-and-counter-insurgency.php>

<sup>113</sup> The Global Terrorism Database (GTD) is an open-source database including information on terrorist events around the world from 1970 through 2011. Its copyrights are under 'The National Consortium for the Study of Terrorism and Responses to Terrorism' (START), which is a Center of Excellence of the U.S. Department of Homeland Security, University of Maryland, College Park, MD, USA. START makes the GTD available online through interface (<http://www.start.umd.edu/gtd/>) in an effort to increase understanding of terrorist violence so that it can be more readily studied and defeated.

total number of incidents by nation. These data show that the major threat for developing countries emerges from insurrections and terrorism.












Name		Count
Colombia		7180
Iraq		6475
India		6114
Peru		6045
El Salvador		5327
Pakistan		4436
Northern Ireland		3885
Spain		3205
Philippines		3191

Figure 13. Temporal trends in terrorism in the Global Terrorism Database (GTD)<sup>114</sup>.

<sup>114</sup> Global Terrorism Database (GTD) website. Accessed November 14, 2012.  
<http://www.start.umd.edu/datarivers/vis/GtdExplorer.swf>

## **2. The IW Capabilities with the Greatest Benefit for Smaller Militaries**

From the preceding discussion, it is evident that the most critical security challenge to developing countries, in general, is the ability to root out insurgencies and terrorist activities. Certain IO capabilities, as delineated in *U.S. Joint Publication 3–13*, like CMO/CA, public diplomacy, PA, PSYOP, MILDEC, and physical attack provide policymakers in such developing countries an effective and viable way of conducting counterinsurgency (COIN) and counterterrorism operations. It is also important to note here that the above-stated capabilities are feasible when considered in the context of using them against an unconventional enemy in an unconventional battlefield. In conventional warfare, employing capabilities such as MILDEC against regular forces will require the latest technological innovations, considerable troops, and financial resources. However, deception when used against insurgents and terrorists will be different and less complex in nature and design. Following this same premise, IW capabilities like EW, CNO and IA typically cannot produce significant direct impacts on the enemy in an asymmetrical environment. Similarly, the enemy in this case is also not typically targeting computer networks and associated infrastructure, because of a relatively limited reliance upon these systems by organizations in developing countries. The primary focus of enemy activities continues to be finding sympathetic local populations and geographical safe havens. The more traditional capabilities of CMO/CA, PA, PSYOP, and MILDEC provide an effective means of controlling the cognitive dimension of the information environment. The ability derived from selected IW capabilities to manage the perceptions of all groups and parties involved in the conflict can significantly contribute to achieving the desired end state.



### **3. Shaping Perceptions with the Help of IW<sup>115</sup>**

As mentioned above, these four capabilities of IO provide the means to monitor and manage the perception of target audiences to meet overall operations objectives. This aim should be kept at the top level and subsequent activity should be regarded as the most important activity of an IO strategy. The highest-level target of IO is the human perception of decision makers, policymakers, military commanders, and even entire populations. The capabilities shown in Figure 14 directly hit these ultimate targets with an objective to influence their perception to affect their decisions and resulting activities.

---

<sup>115</sup> Information in this section is taken by abridging and modifying details from Waltz, *Information Warfare*, 162–165.

Perception Disciplines		Target Audience	Perception Objectives and Means
Military affairs	Public affairs	Friendly forces Media Friendly populations	Objectives: To provide a consistent presentation of accurate, balanced, and credible information that achieves confidence in forces and operations  Means: Press releases, briefings, and broadcasts (radio, TV, net)
	Civil affairs	Foreign civil authorities and population in areas of conflict	Objectives: To provide a consistent presentation of position and credible information that supports friendly objectives  Means: Civil meetings, press releases, briefings, broadcasts (radio, TV, net)
Military perceptions management	Psychological operations (PSYOPS)	Hostile foreign forces Hostile or neutral foreign populations	Objectives: To convey selected information and indicators to foreign audiences to influence emotions, motives, objective reasoning, and, ultimately, to induce behavior to meet objectives  Means: Projection of truth and credible messages via all media
	Military deception	Hostile foreign military leaders  Hostile foreign forces	Objectives: To confuse or mislead enemy leaders to make decisions that cause actions that are exploitable by friendly forces  Means: Deceptive operations, activities, or stories to conceal, distort, or falsify indications of friendly intentions, capabilities, or actions

Figure 14. Capabilities Involved in Shaping Perception.<sup>116</sup>

Public and civil-affairs operations (including civil–military operations) are open, public presentations of the truth (not misinformation or propaganda) in a context and format that achieves perception objectives defined in a perception plan. These are the best tools to counter enemy propaganda (terrorist and insurgent survival rests in the local population’s defection from the government).

<sup>116</sup> Waltz, *Information Warfare*, 163.

PSYOP also convey only selected truthful messages, as described in its definition covered in Chapter III, to foreign audiences (including hostile forces) to influence both the emotions and reasoning of decision makers. Selected themes and emphasis are chosen often in the process along with selected indicators to meet objectives. PSYOP require careful tailoring of the message (to be culturally appropriate) and selection of the media (to ensure that the message is received by the target population). The most appropriate media (method of delivery of the message) in developing countries comes in the forms of direct broadcast television and radio, posters/leaflets, loudspeakers, and telephone conversations. Certain government/military actions, such as preparations for military offensive, also contribute toward PSYOP. Developing of appropriate message themes should be done in consultation with those members of civil/military organizations belonging to the same tribe or ethnicity in order to create the desired perception in the target population. PSYOP efforts should also be directed in places bordering insurgent-infested areas so as to prevent the rest of the population residing in adjoining locations from joining or supporting rebels and winning their support for government actions/military operations. A general model of a PSYOP campaign depicting its functional flow is illustrated in Figure 15.

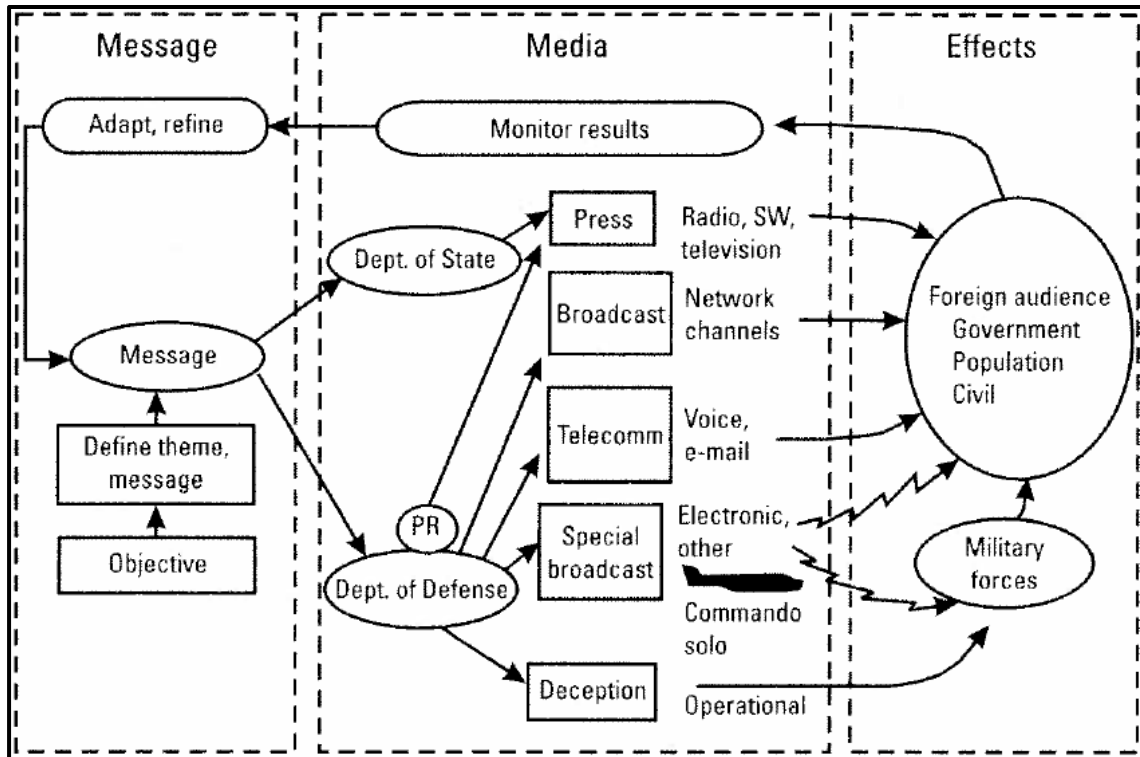


Figure 15. Functional Flow of a PSYOP Campaign.<sup>117</sup>

In contrast to the first three means, military deception operations are performed in secrecy (assisted by operational, physical, and communications security) with the objective of conveying untruthful or inaccurate information to deceive the enemy. These operations are designed to induce hostile leaders to take operational or tactical actions that are favorable to, and exploitable by, friendly combat operations. It is pertinent here that deception contributes to the achievement of a perception objective; it is generally not an end objective in itself. In the case of low-intensity conflict or irregular warfare, planning and execution of deception by a regular military force should be relatively less complicated, inexpensive, and more swiftly executable. In the cases of both PSYOP and MILDEC, intelligence must provide feedback on the degree of efficacy of these efforts in order to introduce timely corrections as necessary.

<sup>117</sup> Waltz, *Information Warfare*, 211.

In addition to the above-mentioned four capabilities that operate mainly in the cognitive dimension, physical attack is an IO-related capability that provides a means in the physical dimension to affect the perceptual level of the enemy and the content and flow of information. The physical components of the information infrastructure (and supporting functions, such as electrical power, air conditioning, and human operators) may be subject to physical attacks to disable (soft kill) or destroy (hard kill) the targeted components. Operational formations and units (e.g., special-operations forces, conventional forces, and attack-aircraft wings of an air force) are assigned physical destruction tasks against the critical command and control nodes of enemy forces. In the battle against insurgency and terrorism, this mode affords execution of the classical maneuver and firepower of the military in support of the information-operations objectives. Intelligence and surveillance resources are required to accurately pinpoint specific locations serving as nerve centers of the enemy communication infrastructure, allowing the use of conventional military means to neutralize these targets expeditiously through surgical strikes. It is pertinent here that these kinetic forces, due to their nature, disposition, and psychological effect, also coordinate with PSYOP and deception operations in synchronization with plans contrived at higher operational levels.

#### **4. A Simplistic Operational Model of Information Warfare<sup>118</sup>**

On the basis of the above discussion, a simplistic operational model of IW can be formed that has general applicability in a developing-country scenario. Consistent with the information-environment discussion covered in Chapter III, where three separate and distinct dimensions (i.e., physical, informational, and cognitive) exist, this model is also based on a corresponding three target areas of IO: physical space, cyberspace, and the minds of humans. The operational model (as represented in Figure 16, below) distinguishes three levels or layers of functions for both the attacker and the target. The layers are hierarchical, with

---

<sup>118</sup> The model is built upon the concept taken from Waltz, *Information Warfare*, 148–151.

influence flowing downward on the attack side and upward on the target side. The objective of the attacker is to influence the target at the perceptual level by actions that may occur at all levels of the hierarchy. For the purpose of this model, the middle (information-structure level) or cyberspace layer will be considered dysfunctional both from attacker and target perspective for the reasons explained earlier in the discussion. CNO against asymmetric forces will not yield any significant outcome in absence of any formal, fully functional information infrastructure in cyberspace and due to a reduced reliance on computer networks. Stringent actions at the perceptual and physical levels can produce much more effective and favorable results for smaller militaries required to overwhelm insurgency and terrorism.

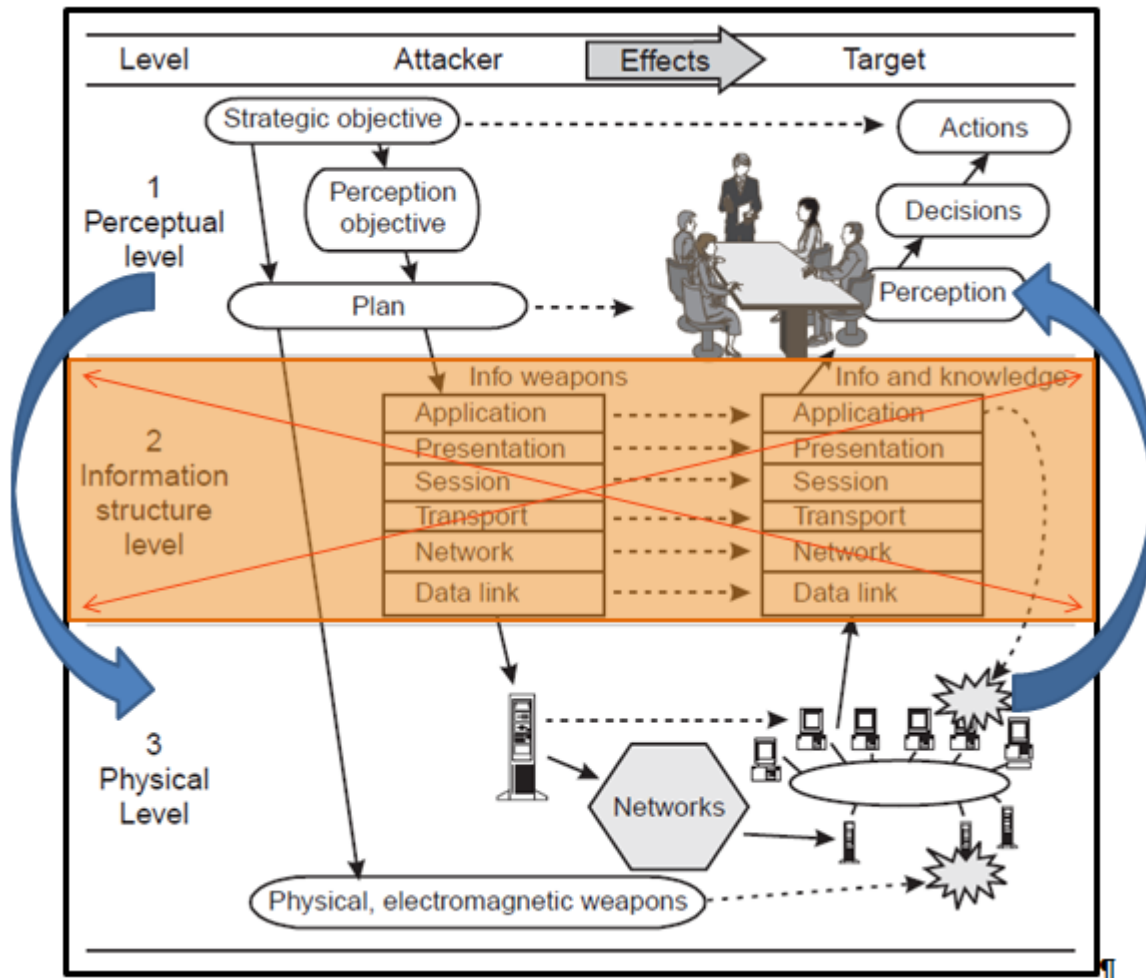


Figure 16. A Simplistic Model for IO in Developing Countries<sup>119</sup>

The first layer is at the perceptual or psychological level, which is abstract in nature and aimed at management of the perception of a target audience. At this level, the strategic objective defines the desired actions of the target and the perception(s) that will most likely cause those actions. If the desired action is termination of aggression, for example, the objective perception for targeted leaders may be “overwhelming loss of control, disarray, and loss of support from the populace.” If the desired action is disengagement from a military action, the objective perception for targeted military commanders may be “lack of logistic support to sustain operations.” These perception objectives may be achieved

<sup>119</sup> Waltz, *Information Warfare*, 149.

through integrated and synchronized employment of a variety of IW capabilities such as physical attack, deception, PSYOP, and PA/CA, as determined earlier. The synergy derived from the timely application of IW capabilities can help influence the operational behavior of the target. This influence can then cause indecision, delay, or decisional bias.

The third and lowest layer is the physical system level, which includes the computers, physical networks, telecommunications, and supporting structural components (e.g., power, facilities, and environmental controls) that implement the information system. Attacks at this layer are physical in nature and involve conventional military forces and weapons. As noted earlier, a smaller military force must be able to proficiently destroy physical targets in order to not only disrupt the information flow in the targeted organization, but also to produce subtle psychological effects. For instance, persistent precision air strikes on the logistics-carrying vehicles of the adversary through effective intelligence, surveillance, and reconnaissance (ISR), besides having effects on physical level through disruption of their supply lines, will also produce favorable results at the perceptual level. The inability to protect and secure supply routes over a period of time may then influence the enemy leadership to capitulate.

#### **D. SUMMARY**

The development of an effective and viable IW capability starts from the top level of national-policy formulation. A comprehensive understanding of the various functional tiers, starting from policy to planning strategies and setting objectives, is mandatory for the political and military leadership at the helm of decision making. Assessment of threats and the operational environment plays a critical role in the development of the strategic plan under the guidelines provided by national security policy. Based on the empirical data, the most prevalent security challenge faced by smaller militaries in developing countries stems from insurgencies and terrorism. In the resulting scenario, militaries are engaged with an unconventional enemy that avoids direct military confrontation and finds



strength in molding and distorting the perceptions of the local populace. Certain traditional military capabilities and activities, coordinated and integrated under the realm of IW, provide a suitable course of action to root out insurrections and terrorism. In this approach, PSYOP, MILDEC, CMO, and PA can provide a means of influence at the perceptual level of the information environment and can seriously degrade or paralyze the decision making of the enemy and affect behavior. On the physical level of the information environment, physical attack provides leverage to military forces to unleash devastating blows that carry far-reaching effects upon the cognitive dimension of the enemy. Prudent planning and coordinated execution of these IW capabilities can make the difference in winning or losing irregular wars.

THIS PAGE INTENTIONALLY LEFT BLANK

## **VI. SUMMARY, RECOMMENDATIONS AND CONCLUSION**

### **A. SUMMARY**

Information warfare is a reality of the 21st century. While the military is focused equally on all dimensions of the information environment—cognitive/perceptual, informational, and physical—non-state-sponsored and business organizations are more inclined to fight a war for information superiority in only the cognitive or perceptual level to achieve their commercial and corporate goals. Information warfare in the context of the military application requires teamwork; it can be seen metaphorically as a handcart with a heavy load. A combined effort from many individuals in a common direction is usually required to pull a heavy cart forward. The required strength of individuals increases as the load gets heavier. In the case of IW, individuals are the various capabilities that must have the synergy and synchronization to produce the desired pulling effect. The peculiar nature of geographical and demographic settings in a country or theater determines the required combination of capabilities and the level of coordination among these like, just as a heavy load on a handcart would require only fit and physically strong individuals to do the arduous pulling.

The study of IW's classification as implemented by the U.S. DoD provides an all-encompassing view of IW capabilities. U.S. IO execution strategy takes into account all possible information avenues that can contribute effectively to achieving mission objectives in general and IO objectives in particular. This line of approach is supported by recent combat experiences in Iraq and Afghanistan, where various IO-related theories have been practically tested in the ruggedness of the battlefield. Similarly, examining the IO organizational structures of the U.S. joint staff and services renders a valuable insight for developing a suitable model in other smaller regional militaries, per the dictates of security challenges.

One of the noticeable differences in the societies of developed and developing countries is the dependence upon information technology in day-to-day affairs. Since most of the commercial, governmental, and military institutions and organizations in developing countries are relatively less reliant on IT and computer networks, they are relatively less vulnerable on this front. Therefore, many of the latest and more technological IO capabilities may make less of a contribution in these countries when seen in the context of fighting against an insurgency or terrorism, their biggest security challenge. On the other hand, an increased focus and coordination on some traditional IW capabilities can bring about extremely favorable results for their efforts. The perceptual and physical dimensions are more apparent and relevant in counterinsurgency and counterterrorism campaigns, and should be exploited prudently. PSYOP and MILDEC (from the core capabilities) along with CMO, public affairs, and public diplomacy (from related capabilities) can be extremely helpful in achieving objectives at the cognitive and perceptual levels. On the physical and kinetic side of operations, physical attack (from supporting capabilities) can be utilized to destroy, disrupt, degrade, and/or deny the physical infrastructure of the enemy. Putting together these capabilities in a cohesive, tenacious, and synchronized manner under the auspices of well thought-out IW strategy presents the best possible and most cost-effective solution for smaller militaries to tackle their biggest security threat. Depending on appreciation of the situation by the decision maker, a comprehensive strategy must articulate the relative priority among the use of capabilities and their extent of application. This will help subordinate commanders to ascertain appropriate scale of the capabilities and place due emphasis in their application, when needed.

## **B. RECOMMENDATIONS**

A general survey of IO capabilities was undertaken in this study with an aim to identifying feasible capabilities that can prove beneficial to the smaller militaries of developing countries. Though the capabilities identified in this process were not examined down to the operational and functional level with

regard to implementation methodology, the understanding obtained hitherto leads to the following recommendations:

### **1. Policy Formulation by Government and Military leaders**

Government and military leaders should focus on developing policies and strategies for conducting and regulating information warfare. In absence of a basic framework provided by such documents, the decision makers normally resort to employ overwhelming conventional force to crush insurgents and terrorists. This practice may yield some success at tactical levels but remains largely ineffective in the long run. Moreover, this heavy-handed tactic also produces heavy collateral damage, thereby alienating local populations, which goes against the objective of counterinsurgency. Employing a combination of non-kinetic IW capabilities in unison with conventional maneuver, as identified in the IW strategy, provides the best course of action in such scenarios.

### **2. Making Comprehensive IW strategy**

A comprehensive IW strategy should involve representations from political leadership (both national and local), civil administration, and the military. Any activity performed without including any of these segments will not address the root causes of instability or conflict. The ambit of civil–military operations suffers serious limitations when a vacuum of civil order exists in the affected area and all powers are exercised by military forces. The CMO and PA staffs should be fully conversant in broader IO plans and objectives. They should try to improve public perceptions in their favor, especially among the masses of their immediate locale, starting with the early stages of a conflict. As a guiding principle, the military should endeavor to contact, not control, the local population.

### **3. Managing the Perceptual Level through IW**

At the perceptual level, it is typically easier for enemy forces to arouse public sentiments against a military presence in an area. PSYOP, CMO, and civil-affairs team should provide full support to legitimate local government

authorities and assist in their functions without interfering with their governance. Any effort by the insurgents and terrorists to challenge the writ of local government must be quelled through the cumulative effect of identified IW capabilities. Due to their very nature, military forces lack permanence in their area of operations. An early restoration of civil order provides a serious blow to enemy agendas and paves the path toward success.

#### **4. Systematic Development of IW Capabilities**

IW capabilities, if properly furthered and developed through regular training and career progression, can transform a military force into a hybrid force. It can then undertake counterinsurgency and counterterrorism operations efficiently besides regular conventional military operations while maintaining a much-desired conventional-military posture. Adequate funding, resources, and staff must be allocated to PSYOP, CMO, and PA teams to train and equip properly before any deployment.

#### **5. Organizing CMO, PSYOP and PA**

CMO, PSYOP and PA teams should maintain continuous liaison with print and electronic media. Their messages and themes should undergo the shortest possible approval process because a late product loses its effectiveness and relevance. Another important point in this regard is performing an advanced planning of PSYOP and PA activities and their continuous updating as diplomatic, political, and military circumstances change frequently during a campaign or conflict. Their charter of duties and action plan for rebuilding and rehabilitation during the post conflict period should be fully worked out at the operational planning level. Any laxity in effort at this stage can severely undermine public support for both the government and the military.

#### **6. Cooperation and Coordination**

The importance of cooperation and coordination among various IW capabilities and agencies entrusted with the execution of those capabilities needs

no further emphasis. A sound strategy and a well-orchestrated plan can be in vain due to a lack of synchronization and timing. All possible channels to share information between various agencies, stakeholders, and IW teams must be established and tested before the commencement of operations. It must be noted here that often the desired outcome of an IW effort is a cumulative product, not just the sum of various information operations, where a single null can bring the entire product to zero.

### **C. CONCLUSION**

The instruments of battle are valuable only if one knows how to use them.

Colonel Charles Ardant du Picq,  
French Army<sup>120</sup>

There are no ready-made solutions for the security challenges of a country. Instead of finding a silver bullet, the correct approach to address national-security issues starts from identifying one's own strengths and vulnerabilities in a realistic and unbiased manner. Based on these findings and analysis, formulation of the appropriate policy and strategy can ultimately lead to effective planning at the operational level. Unfortunately, in many developing countries, due attention is not rendered toward formulation of policies, strategies, and doctrines, which results in a void of directivity at the executional level. The situation is not different either when it comes to harnessing potentials on the informational front. The U.S. information-operations model provides suitable guidelines for exploiting the powers of information. It is up to national policy and decision makers to treat information as an instrument of national power on diplomatic, economic, and military lines, or consider it in a support function for other national elements. The later approach will limit the information scope as a leveraging force required in the success of campaigns, battles, and conflicts. From U.S. doctrine, it is apparent that certain traditional military disciplines,

---

<sup>120</sup> Charles Ardant du Picq, *Battle Studies: Ancient and Modern Battle*, 8th ed. (French), trans. John Greely and Robert C. Cotton (New York: Macmillan, 1920).

upgraded and modified for modern-day use, provide an effective means to manipulate enemy perceptions at tactical, operational, and strategic levels, thus undermining greatly the enemy's capacity to wage and sustain war. IO capabilities of PSYOP, CMO, PA, and MILDEC, if properly developed and employed, can be extremely useful at the perceptual level of the information environment. These capabilities, coupled with timely targeting of carefully selected communication hubs and infrastructure through physical attack, can create paralysis in the enemy's organization, resulting in his capitulation.



## **APPENDIX A. U.S. UNIFIED COMMAND PLAN (UCP) AND COMBATANT COMMANDS (COCOMS)**

The Unified Command Plan (UCP) and associated combatant commands (COCOMS) provide operational instructions and command and control to the armed forces and have a significant impact on how they are organized, trained, and resourced—areas over which Congress has constitutional authority. In a grand strategic sense, the UCP and the COCOMs are the embodiment of U.S. military policy both at home and abroad. The COCOMs not only execute military policy but also play an important role in foreign policy.<sup>121</sup>

### **A. COMBATANT COMMAND (COCOM)**

DoD defines combatant command (COCOM) as “a unified<sup>122</sup> or specified<sup>123</sup> command with a broad continuing mission under a single commander established and so designated by the president, through the secretary of defense and with the advice and assistance of the chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities.<sup>124</sup>

Commands are in charge of utilizing and integrating air, land, sea, and amphibious forces under their commands to achieve U.S. national security objectives while protecting national interests. Three of the unified commands

---

<sup>121</sup> Andrew Feickert, “The Unified Command Plan and Combatant Commands: Background and Issues for Congress,” Congressional Research Service Report, July 17, 2012: 1.

<sup>122</sup> Joint Publication 1–02 defines a unified command as a “command with a broad continuing mission under a single commander and composed of significant assigned components of two or more Military Departments that is established and so designated by the President, through the Secretary of Defense with the advice and assistance of the Chairman of the Joint Chiefs of Staff.”

<sup>123</sup> Joint Publication 1–02 defines a specified command as “a command that has a broad, continuing mission, normally functional, and is established and so designated by the President through the Secretary of Defense with the advice and assistance of the Chairman of the Joint Chiefs of Staff. It normally is composed of forces from a single Military Department.”

<sup>124</sup> *Ibid.*, 52.

handle functional concerns while there are six with geographic mandates. The specific configurations have shifted over the decades, but the idea that geography provides an organizing principle remains the same, allowing each combatant command to have its specific threats and opportunities. The combatant commanders work with the military forces in their theaters, and report to the commander in chief and secretary of defense. The combatant commanders do not serve on the Joint Chiefs of Staff nor are they the senior U.S. representatives in the theater.<sup>125</sup> The number of combatant commands is not regulated by law or policy and their numbers and responsibilities have varied over the years. Today, there are nine active COCOMs, with one COCOM, U.S. Joint Forces Command (JFCOM), disestablished in August 2010 and all of its remaining functions transferred to other COCOMs or organizations.<sup>126</sup>

The nine COCOMs are briefly discussed here:<sup>127</sup>

## **1. Functional Combatant Commands**

Functional combatant commands operate worldwide across geographical boundaries and provide unique capabilities to geographic combatant commands and the services:

- USSOCOM: U.S. Special Operations Command, MacDill Air Force Base, Florida;
- USSTRATCOM: U.S. Strategic Command, Offutt Air Force Base, near Omaha, Nebraska; and
- USTRANSCOM: U.S. Transportation Command, Scott Air Force Base, Illinois.

---

<sup>125</sup> Cynthia A. Watson, "Combatant Commands: Origins, Structure, and Engagement," Praeger Security International, 2011: 15.

<sup>126</sup> Feickert op. cit., 2.

<sup>127</sup> Ibid.

## **2. Geographic Combatant Commands**

Geographical combatant commands operate in clearly delineated areas of operation and have a distinctive regional military focus.

- USAFRICOM: U.S. Africa Command, Kelley Barracks, Stuttgart, Germany;
- USCENTCOM: U.S. Central Command, MacDill Air Force Base, Florida;
- USEUCOM: U.S. European Command, Patch Barracks, Stuttgart, Germany;
- USNORTHCOM: U.S. Northern Command, Peterson Air Force Base, Colorado;
- USPACOM: U.S. Pacific Command, Camp H.M. Smith, Hawaii; and
- USSOUTHCOM: U.S. Southern Command, Miami, Florida.



Figure 17. U.S. COCOMS Area of Responsibility in 2011<sup>128</sup>.

### 3. Command Authority

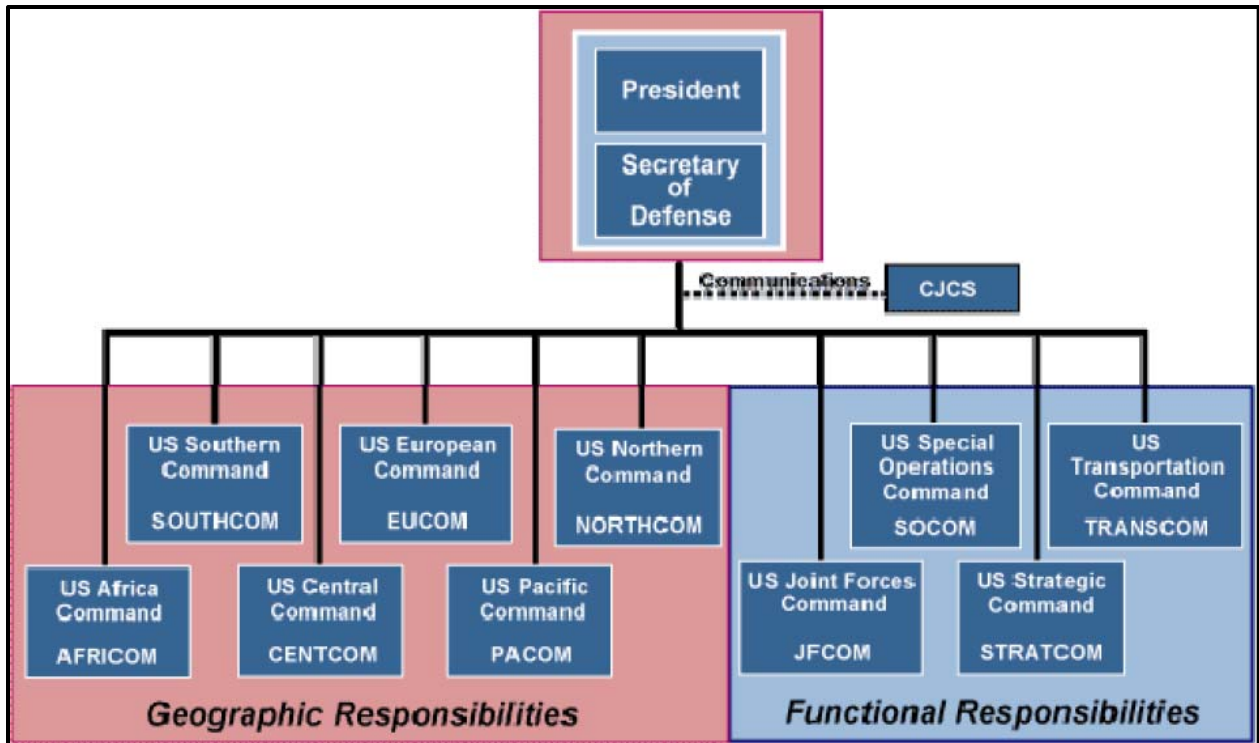
The structure of command authority should be of particular interest as democratic representatives of the United States exercise direct control over strategic and operational military commands. Forces assigned to COCOMs are under the command of that COCOM commander, with the chain of command starting with the President and running through the Secretary of Defense (SecDef) as indicated in Figure 3. The CJCS serves as a link between the President and the SecDef and the COCOM commanders. The President can send guidance to COCOM commanders through the Chairman of the Joint Chiefs of Staff (CJCS), and the Chairman can relay combatant commander's needs and concerns to the SecDef and the President. The CJCS may exercise

<sup>128</sup> U.S. Department of Defense website. Accessed October 26, 2012.  
[http://www.defense.gov/home/features/2009/0109\\_unifiedcommand/](http://www.defense.gov/home/features/2009/0109_unifiedcommand/)

oversight of the COCOMs, if desired by the SecDef, but has no command authority over the COCOMs. In this regard, the CJCS is described as taking part in national security discussions but not in the formal decision-making process as it relates to COCOMs.<sup>129</sup>

---

<sup>129</sup> Feickert op. cit., 11.



Note: USJFCOM was disestablished in August 2010 and no longer functions as a COCOM.

Figure 18. U.S. COCOMS Chain of Command<sup>130</sup>

#### 4. Organizational Principles<sup>131</sup>

COCOM commanders hold four-star flag rank and have risen through the ranks of their respective services, commanding at the highest levels. COCOM commanders have also met joint military education requirements as set forth in the Goldwater-Nichols Act. The President nominates combatant commanders based on the recommendations of the SECDEF. The Senate Armed Services Committee holds confirmation hearings for the nominees and the Senate then votes to confirm the candidates. While four-star officers from any service may serve as combatant commander for any given COCOM, some appointments (e.g., U.S. Pacific Command being commanded by a Navy admiral) traditionally

<sup>130</sup> Ibid.

<sup>131</sup> Ibid., 13–14.

have gone to specific services. The basic configurations of COCOM staffs are generally the same and mirror the Joint Staff at the Pentagon. COCOM staffs are organized as follows, although there are variations based on unique COCOM mission areas:

- J-1 Directorate of Manpower and Personnel;
- J-2 Directorate of Intelligence;
- J-3 Directorate of Operations;
- J-4 Directorate of Logistics;
- J-5 Directorate of Strategic Plans and Policy;
- J-6 Directorate of Command, Control, Communication, and Computer;
- J-7 Directorate of Operational Planning and Joint Force Development;
- J-8 Directorate of Force Structure, Resources, and Assessment;  
and
- J-9 Directorate of Interagency Partnering.

Within the COCOM command and staff construct, joint task forces (JTFs) are often created to address a single policy concern and allocate resources, such as anti-drug efforts or humanitarian assistance, on a short to midterm basis. JTFs can also be established in response to a crisis or for a long-term commitment.

THIS PAGE INTENTIONALLY LEFT BLANK



## **APPENDIX B. U.S. STRATEGIC COMMAND'S SUBCOMPONENTS**

### **A. FUNCTIONAL COMPONENTS<sup>132</sup>**

#### **1. U.S. Cyber Command (USCYBERCOM)**

USCYBERCOM, under the command of a four-star flag officer, is subordinate to USSTRATCOM. It plans, coordinates, integrates, synchronizes, and conducts activities to defend U.S. DoD information networks and also conducts cyber space activities to enable U.S. military activities. Organization of USCYBERCOM includes following service elements

- USA—Army Cyber Command (ARFORCYBER/2nd Army)
- USAF—Air Force Cyber Command (AFCYBER/24th AF)
- USN—Fleet Cyber Command (FLTCYBERCOM/10th Fleet)
- USMC—Marine Forces Cyber Command (MARFORCYBER)

#### **2. Joint Functional Component Command—Global Strike (JFCC-GS)**

JFCC-GS optimizes planning, integration, execution and force management of assigned missions to deter attacks against the United States, its territories, possessions, and bases.

#### **3. Joint Functional Component Command—Space (JFCC-Space)**

JFCC-Space is responsible for executing continuous, integrated space operations to deliver theater and global effects in support of national and combatant commander objectives.

---

<sup>132</sup> Information in this section is taken from 132 Feickert op. cit., 21–22 and USSTRATCOM official website. Accessed November 3, 2012. [http://www.stratcom.mil/functional\\_components/](http://www.stratcom.mil/functional_components/)

**4. Joint Functional Component Command–Integrated Missile Defense (JFCC-IMD)**

JFCC-IMD synchronizes operational-level global missile defense planning, operations support, and the development of missile defense effects for DoD.

**5. Joint Functional Component Command–Intelligence, Surveillance and Reconnaissance (JFCC-ISR)**

JFCC-ISR plans, integrates, and coordinates intelligence, surveillance and reconnaissance in support of strategic and global operations and strategic deterrence.

**6. USSTRATCOM Center for Combating Weapons of Mass Destruction (SCC–WMD)**

SCC–WMD plans, advocates, and advises the USSTRATCOM commander on WMD-related matters.

**7. Joint Warfare Analysis Center (JWAC)**

JWAC is a premier science and engineering institution tasked with solving complex challenges for U.S. warfighters. JWAC coordinates directly with the staffs of all unified commands, combatant commands, Department of Defense (DoD) elements, military services, and other government departments and agencies in order to protect U.S. and help its armed forces accomplish their missions.

**B. SERVICE COMPONENTS<sup>133</sup>**

**1. Air Force Global Strike Command (AFGSC)**

AFGSC is responsible for the Air Force's three intercontinental ballistic missile (ICBM) wings, two B-52 Stratofortress wings and the sole B-2 Spirit wing. AFGSC has two numbered air forces that are tasked with providing capabilities to

---

<sup>133</sup> Information in this section is taken from Feickert op. cit., 20–21 and USSTRATCOM official website. Accessed November 3, 2012. [http://www.stratcom.mil/service\\_components/](http://www.stratcom.mil/service_components/)

combatant commands. The Eighth Air Force controls the long-range nuclear bomber assets (B-52s and B-2s) and the Twentieth Air Force controls the ICBM wings.

## **2. U.S. Army Forces Strategic Command (ARSTRAT)**

ARSTRAT conducts space and missile defense operations and provides planning, integration, control, and coordination of Army forces and capabilities in support of USSTRATCOM missions.

## **3. Fleet Forces Command**

Fleet Forces Command is responsible for the entire Atlantic Ocean, the Caribbean Sea, and the waters around Central and South America extending into the Pacific to the Galapagos Island.

## **4. Marine Corps Forces U.S. Strategic Command (MARFORSTRAT)**

MARFORSTRAT serves as the Marine Corps service component to USSTRATCOM.

## **5. Air Force Space Command (AFSPC)**

AFSPC provides space and cybersecurity forces for USSTRATCOM. It has two numbered air forces providing these capabilities. The Fourteenth Air Force controls and supports several satellite systems including the Global Positioning System (GPS); Defense Satellite Communications Systems Phase II and III; and the Defense Meteorological Support Program. In addition, the Fourteenth Air Force has Atlas, Delta, and Titan launch vehicles at its disposal to put payloads into orbit. The Twenty-Fourth Air Force plans and conducts cyberspace operations in support of combatant commands.

THIS PAGE INTENTIONALLY LEFT BLANK

## **APPENDIX C. U.S. SPECIAL OPERATIONS COMMAND'S SUBCOMPONENTS**

USSOCOM consists of four component commands and one sub-unified command. Their brief description is given hereunder:<sup>134</sup>

### **1. U.S. Army Special Operations Command (USASOC)**

USASOC is the largest of the service components that make up USSOCOM and provides about 70 percent of the special operations personnel in Central Command's theatre. It includes Army Special Forces, also known as Green Berets; Rangers; civil affairs, and military information support operations (MISO) units. In addition, the 160th Special Operations Aviation Regiment (SOAR) provides rotary-wing support to all SOF units. USASOC forces include:

- 4th MISO Group (Airborne) (4th MISOG)
- 8th MISO Group (Airborne) (8th MISOG)
- 95th Civil Affairs Brigade (Airborne)
- United States Special Forces Command (Airborne).
- John F. Kennedy Special Warfare Center and School.
- 75th Ranger Regiment
- United States Army Special Operations Aviation Command
- 160th Special Operations Regiment (Airborne)
- 528th Sustainment Brigade (Airborne)

### **2. Naval Special Warfare Command (NSWC)**

NSWC consists of Sea, Air, and Land (SEAL) teams that conduct operations in both maritime and ground environments. NSWC also has SEAL delivery vehicle (SDV) teams—specialized SEALs that pilot small submersible

---

<sup>134</sup> Information in this section is taken from USSOCOM website <http://www.socom.mil/default.aspx> and U.S. Army War College IO Primer, November 2011, 146–147 and Feickert op. cit., 16–18.

vehicles that can deliver SEALs to their area of operations. NSWG includes special boat teams that can deliver SEALs from ship to shore as well as operate in the littorals and rivers.

### **3. Air Force Special Operations Command (AFSOC)**

AFSOC provides specialized fixed and rotary wing support to USSOCOM units. In addition to aircraft support, AFSOC also provides combat controllers, para-rescue jumpers, Special operations weather teams, and tactical air control parties (TACPs) to support special operations. AFSOC is currently establishing a capacity to train and advise partner nation aviation units as part of foreign internal defense initiatives.

### **4. Marine Special Operations Command (MARSOC)**

Established in 2005, MARSOC is the newest USSOCOM subcomponent. It consists of three Marine special-operations battalions, a Marine special-operations support group, a Marine special-operations intelligence battalion, and the Marine Special Operations School.

### **5. Joint Special Operations Command (JSOC)**

A sub-unified command of USSOCOM, JSOC provides a joint headquarters to study special operations requirements, ensures interoperability and equipment standardization, develops joint special-operations plans and tactics, and conducts joint special-operations exercises and training.

## LIST OF REFERENCES

### A. LITERATURE

- Ardant du Picq, Charles. *Battle Studies: Ancient and Modern Battle*, 8th ed. (French), trans. John Greely and Robert C. Cotton. New York: Macmillan, 1920.
- Armistead, Edwin Leigh and Murphy, Thomas. *The Evolution of Information Operations Contracts across the DoD: Growth Opportunities for Academic Research*. Proceedings of the 2<sup>nd</sup> International Conference on Information Warfare and Security, March 2007.
- Beavers, Garry J. Lieutenant Colonel U.S. Army, Retired. *Defining the Information Campaign*. Military Review November-December 2005.
- Duke, Cynthia R. *Bridging the Gap in the Realm of Information Dominance: a Concept of Operations for the Naval Postgraduate School Center for Cyber Warfare*. Naval Postgraduate School Thesis, September 2010.
- Franz, Timothy P. Durkin, Matthew F. Williams, Paul D. Raines, Richard A. Mills, Robert F. *Defining Information Operations Forces*. Air & Space Power Journal Summer 2007.
- Feickert, Andrew. "The Unified Command Plan and Combatant Commands: Background and Issues for Congress." *Congressional Research Service Report*, July 17, 2012: 1.
- Gilmer, Carter. *The Future of Information Warfare*. SANS Institute GSEC Practical Assignment Version 1.2f, 2001.
- Griffith, Samuel B. *Sun Tzu: The art of War*. London: Oxford University Press, 1963.
- Ventre, Daniel. *Information Warfare*. London: ISTE Ltd, 2009.
- Waltz, Edward. *Information Warfare Principles and Operations*. Boston: Artech House Publications, 1998.
- Watson, Cynthia A. "Combatant Commands: Origins, Structure, and Engagement." *Praeger Security International*, 2011: 15.

### B. MILITARY PUBLICATIONS

- United States Air Force Doctrine Document (AFDD) 2–5. *Information Operations*. January 2005.

- United States Department of Defense Directive (DODD) number 3600.01  
*Information Operations*, May 2011.
- United States Department of Defense Directive (DODD) number 7045.20,  
*Capability Portfolio Management*, September 2008.
- United States Marine Corps Bulletin 5400. *Establishment of MCIOC Phase One*.  
Washington DC, March 2008.
- United States Marine Corps Order 3120.10. *Marine Corps Information  
Operations Program (MCIOP)*. June 2008.
- United States Marine Corps Warfare Publication MCWP 3–40.4. *Marine Air-  
Ground Task Force Information Operations*. July 2003.
- United States National Defense University Armed Forces Staff College. *The Joint  
Staff Officer's Guide 1997*. Norfolk, Virginia, 1997.
- United States Navy Magazine, Anchor Watch. *CNO stands up Fleet Cyber  
Command*. March 2010.
- United States. Department of the Army Field Manual (FM) 100–7. *“Decisive  
Force: The Army in Theater Operations.”* Washington, DC, May 1995.
- United States. Department of the Army Field Manual (FM) 3–13. *“Inform and  
Influence Activities- Final Draft.”* Washington, DC, October 2011.
- United States. Department of the Navy, Chief of Naval Operations for  
Information, Dominance. *U.S. Navy's Vision for Information Dominance*,  
Washington, DC, 2010.
- United States. Secretary of Defense Memorandum, *Strategic Communication  
and Information Operations in the DoD*, Washington D.C.: Department of  
Defense, January 2011.
- United States. U.S. Army War College Information Operations Primer.  
*Fundamentals of Information Operations*. Pennsylvania, 2011.
- United States. U.S. Joint Chief of Staff, Joint Publication 1–02. *Department of  
Defense Dictionary of Military and Associated Terms*. Washington, DC,  
2011.
- United States. U.S. Joint Chief of Staff, Joint Publication 3–13. *Joint Doctrine for  
Information Operations*. Washington, DC, 2011.



### C. INTERNET SOURCES

- Global Terrorism Database (GTD) website. Accessed November 14, 2012.  
<http://www.start.umd.edu/datarivers/vis/GtdExplorer.swf>
- Graves, Rodney. "A short course in the history of insurgency and counter-insurgency." Accessed November 15, 2012.  
<http://wizbangblog.com/content/2011/06/01/a-very-short-course-in-the-history-of-insurgency-and-counter-insurgency.php>
- Grover, Amit. "Cyber War's Final Frontier: Network Centric Warfare Framework." Accessed June 25, 2012, [http://www.itffroc.org/articles/ag\\_cyberwar.pdf](http://www.itffroc.org/articles/ag_cyberwar.pdf)
- Hali, Sultan M Group Captain. "The role of media in war." *Defence Journal* (2000). Accessed June 5, 2012.  
<http://www.defencejournal.com/2000/aug/role-media-war.htm>
- Hume, Bob Col. "DoD Education 2009." Accessed October 31, 2012.  
<https://dde.carlisle.army.mil/documents/courses.../ppt/2208-UCP.ppt>
- Josten, Richard J. "Strategic Communication: Key Enabler for Elements of National Power." *IOSPHERE* (Joint Information Operations Center), Summer 2006. Accessed November 2, 2012.  
[http://www.carlisle.army.mil/DIME/documents/iosphere\\_summer06\\_josten.pdf](http://www.carlisle.army.mil/DIME/documents/iosphere_summer06_josten.pdf)
- Online article. "N2/N6 Reorganization." Accessed November 6, 2012.  
<http://www.dawnbreaker.com/portals/p3p/opnav/opnav-n2-n6.php>
- Rajan, Raghu Air Marshal. "Impact of Information Warfare on Aerospace Operations." *IDR Issue Vol 26.2* Apr-Jun 2011. Accessed June 4, 2012, <http://www.indiandefencereview.com/interviews/impact-of-information-warfare-on-aerospace-operation>
- Reider, Bruce J. "Strategic Realignment: Ends, Ways, And Means In Iraq." *The U.S. Army professional writing collection*. Accessed November 2, 2012.  
[Http://www.army.mil/professionalwriting/volumes/volume6/february\\_2008/2\\_08\\_3.html](Http://www.army.mil/professionalwriting/volumes/volume6/february_2008/2_08_3.html)
- Simmons, Rob. "Information Operations: All Information, All Languages, All the Time." Accessed November 02, 2012.  
[http://www.google.com/url?sa=t&rct=j&q=is%20io%20part%20of%20dime&source=web&cd=5&cad=rja&ved=0CDIQFjAE&url=http%3A%2F%2Fwww.oss.net%2Fdynamaster%2Ffile\\_archive%2F051109%2Faf481ac312ef876d0fab0965a09b28df%2F004%2520Body%2520of%2520Book%2520with%2520Footnotes.doc&ei=mxeUUL-wOaG4igLb3oGQDg&usg=AFQjCNHU9\\_Cg8lby-tyBLjEbLSVJMeM\\_uw](http://www.google.com/url?sa=t&rct=j&q=is%20io%20part%20of%20dime&source=web&cd=5&cad=rja&ved=0CDIQFjAE&url=http%3A%2F%2Fwww.oss.net%2Fdynamaster%2Ffile_archive%2F051109%2Faf481ac312ef876d0fab0965a09b28df%2F004%2520Body%2520of%2520Book%2520with%2520Footnotes.doc&ei=mxeUUL-wOaG4igLb3oGQDg&usg=AFQjCNHU9_Cg8lby-tyBLjEbLSVJMeM_uw)

- Space and Naval Warfare Systems Command, "Making the Navy's Information Dominance Vision a Reality. Accessed October 23, 2012.  
[http://www.public.navy.mil/spawar/Press/Documents/Publications/1.18.12\\_AFCEA\\_Kit\\_II.pdf](http://www.public.navy.mil/spawar/Press/Documents/Publications/1.18.12_AFCEA_Kit_II.pdf) on
- The disastrous "Desert One" Rescue Operation. Accessed November 4, 2012.  
<http://www.freerepublic.com/focus/f-news/547308/posts>
- The U.S. Navy Vision for Information Dominance, May 2010: 2–4 retrieved from  
<http://www.insaonline.org/assets/files/NavyInformationDominanceVisionMay2010.pdf> on October 22, 2012.
- The U.S. Navy Vision for Information Dominance, May 2010: 9. Accessed October 22, 2012.  
<http://www.insaonline.org/assets/files/NavyInformationDominanceVisionMay2010.pdf> on October 22, 2012.
- The U.S. Navy website. "CNO realigns OPNAV Staff." Accessed November 6, 2012. [http://www.navy.mil/submit/display.asp?story\\_id=65845](http://www.navy.mil/submit/display.asp?story_id=65845).
- The United States Special Operations Command official website. Accessed November 17, 2012. <http://www.socom.mil/default.aspx>
- U.S. Cyber Command Fact Sheet published by U.S. DoD Office of the Public Affairs. Accessed November 17, 2012. [http://www.defense.gov/home/features/2010/0410\\_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf](http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf)
- U.S. Marine Corps Document. "Attachment I Interservice Support Agreement #M00264–09098–409." Accessed October 30, 2012.  
[www.quantico.usmc.mil/download.aspx?Path=./Uploads/Files/...](http://www.quantico.usmc.mil/download.aspx?Path=./Uploads/Files/...)
- U.S. Strategic Command official website. Accessed October 28, 2012.  
<http://www.stratcom.mil/about/>
- Whitehead, Yulin. "Information as a Weapon: Reality versus Promises." *Airpower Journal* Fall 1997:50. Accessed November 15, 2012. [ics-www.leeds.ac.uk/papers/pmt/exhibits/548/whitehead.pdf](http://ics-www.leeds.ac.uk/papers/pmt/exhibits/548/whitehead.pdf)
- Wik, Manuel W. "Revolution in Information Affairs." Tactical and Strategic Implications of Information Warfare and Information Operations: 14. Accessed July 3, 2012, doi: 10.1.1.196

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Professor Dan Boger  
Chair, Department of Information Science  
Naval Postgraduate School  
Monterey, California
4. Academic Associate Steve Iatrou  
Naval Postgraduate School  
Monterey, California
5. Lecturer Edward Fisher  
Naval Postgraduate School  
Monterey, California